BIG DATA IN DE ZORG

VERENIGING VOOR GEZONDHEIDSRECHT

BIG DATA IN DE ZORG

Deel 1 – Gegevenszee en het privacybegrip

Wat is big data?
L. OTTES, ARTS
Big data en privacy. Luctor et emergo?
MR. P.M. KITS

Deel 2 – Controle en toezicht op gebruik van big data

Privacyrisico's en -waarborgen bij het gebruik van big data tegen zorgfraude: een verkenning
PROF. MR. G.J. ZWENNE EN MR. DR. DRS. W.A.M. STEENBRUGGEN

Deel 3 – Big data en zorginstellingen

Big data voor een lerend zorgsysteem
MR. E.B. VAN VEEN
De juridische uitdagingen voor een zorginstelling bij big data
MR. T.G. KLEEFMAN

Deel 4 – Big data en wetenschappelijk onderzoek

Big data en open science
PROF. DR. F. MIEDEMA
Big data, medisch-wetenschappelijk onderzoek en gegevensbescherming
MR. M. MOSTERT

Preadvies uitgebracht voor de Vereniging voor Gezondheidsrecht,
jaarvergadering 31 maart 2017

Sdu Uitgevers
Den Haag, 2017

Meer informatie over deze en andere uitgaven kunt u verkrijgen bij:
Sdu Klantenservice
Postbus 20014
2500 EA Den Haag
tel.: 070 - 378 9880
e-mail: sdu@sdu.nl
www.sdu.nl/klantenservice

ISBN 978 90 12 39949 4
NUR 822

WOORD VOORAF

Big data in de zorg

Er zijn revoluties die opvallender verlopen, maar de dataficatie[1] van de samenleving en daarmee van de zorg, mag zeker zo genoemd worden. Wij leven allang in een informatiesamenleving, waarin data als 'het nieuwe goud' of 'de nieuwe olie' worden beschouwd.[2] Nu is het adagium 'kennis is macht' (Francis Bacon) al heel oud en 'intelligence' altijd al een beslissende factor in politiek, handel en business geweest. Met de huidige informatisering is er echter een nieuwe vloed aan data beschikbaar gekomen door registraties, screening, sensoren, waarop de gemiddelde burger allang het zicht is kwijtgeraakt, maar waarmee bedrijven, instellingen en overheid nieuwe informatie en strategieën verwerven. Onze privacywetgeving en het beroepsgeheim in de zorg zijn gebaseerd op de vertrouwde gedachte van overzichtelijke en beheersbare datasets, in de zorg bijvoorbeeld een registratie van NAW-gegevens en het burgerservicenummer, een verslag, een foto, de lab-uitslag en de brieven met andere hulpverleners en dergelijke, die tezamen het medisch dossier vormen. Data zijn echter zo langzamerhand overal door de alom aanwezige technologie, die op deze gegevens draait en deze ook genereert. Deze grondstof geeft onverwachte mogelijkheden, ook wat betreft gezondheidsgegevens. Een sprekend voorbeeld: via de creditcard met een *loyalty scheme* (soort AH-bonuskaart) wist een Amerikaanse supermarkt op basis van koopgedrag eerder dat dochter van 16 zwanger was (en zond haar aangepaste aanbiedingen) dan haar (daarover klagende) vader.[3] Google – zo wil het verhaal[4] – zag de verspreiding van de griepepidemieën twee weken eerder dan overheidsinstellingen, doordat het zoekgedrag volgde van gebruikers die met bepaalde symptomen op internet op zoek gingen naar een diagnose. Op uw iPhone houdt een stappenteller bij hoeveel u beweegt (als u de iPhone meeneemt) en zet het in de iCloud als u niet oppast. Steeds meer sensoren zullen we in de domotica gaan inzetten en daarmee actief voortdurend gezondheidsgegevens genereren. Alle medische scans bevatten veel meer informatie dan benut is voor het ene controlepunt waarvoor ze toevallig zijn gemaakt. Tezamen met alle elektronische patiëntendossiers zijn dat goudmijnen aan onderzoeksdata (*function creep*). De dataopslag vraagt zo veel

---

1 G.J. Zwenne, 'De onbestaanbare olifant: de gedachten over Big Data en de Privacywet', *Tijdschrift voor Internetrecht*, 2015, nr. 4, p. 142-147, m.n. p. 142-143.

2 N. Wolters Ruckert & L. van Sloten, 'Big Data: Privacy Challenges', *Computerrecht* 2016/82.

3 Zwenne 2015, p. 144.

4 Zo opent het boek *De Big Data Revolutie. Hoe de data-explosie al onze vragen gaat beantwoorden* van V. Mayer-Schönberger & Kenneth Cukier, Amsterdam: Maven Publishing 2013/2016 (8ste druk), p. 8-10.

hardware en software, dat zij buiten de instellingen gaan worden bewaard in datacenters of datawarehouses. Er ontstaan zo en door sensoren of met internet verbonden apparatuur (*the Internet of Things*) steeds meer reservoirs aan gegevens, deels realtime beschikbaar, ofwel *big data*.
Het gebruik van big data is buiten de zorg al niet meer tegen te houden. Dat willen we ook helemaal niet. De overheid zet in op het intensiveren van de opleiding van datascientists, opdat wij internationaal de boot niet missen.[5] Op de Nationale Wetenschapsagenda is voor big data een afzonderlijke route onderscheiden.[6] De Wetenschappelijke Raad voor het Regeringsbeleid en het WODC brachten reeds een verkenning uit over de betekenis, kansen en risico's van big data.[7] Op het internet blijkt de term 'big data' zelf al big data te generen.[8]
Als big data daarbij een hele uitdaging voor de privacywetgeving in het algemeen vormt,[9] dan temeer zo in de zorg. Vijf uitgangspunten van de klassieke privacybescherming worden bij big data wel ter discussie gesteld of tot 'mythe' verklaard: de mythe van het anonieme karakter van big data (herleidbaarheid tot personen), de mythe van de doelbinding (zogenoemde *function creep*; zie art. 7 Wbp), de mythe van de dataminimalisering: slechts gegevens verwerken voor zover 'noodzakelijk' (art. 8 Wbp) en niet 'bovenmatig'(art. 11.1 Wbp), de mythe van de toestemming en transparantie (art. 8 aanhef en onder a Wbp) en de mythe van de beveiliging van data (art. 13 Wbp).[10] Big data lijkt op deze manier uitdrukking van een *disruptive technology*, waarbij de bekende wereld op de schop gaat door nieuwe technieken. Voor de zorgsector waar privacy en het beroepsgeheim tot de centrale waarden behoren, is dat een extra bedreiging. Wat betekent big data voor de zorg?
In de preadviezen voor de jaarvergadering 2017 verkennen wij het terrein van de big data voor de zorg nader:

Deel 1 van de preadviezen 'Gegevenszee en het privacybegrip' gaat over de contouren van big data in de maatschappij en de zorg. Leo Ottes, arts en mr. Peter Kits nemen dit deel voor hun rekening en verschaffen ons een begrip van wat big data is (Ottes) en de daarbij spelende fundamentele privacyproblemen (Kits).

In deel 2 'Controle en toezicht op gebruik van big data' gaan prof. mr. Gerrit-Jan Zwenne en dr. Wilfred Steenbruggen in op de fraudecontrole met behulp van big

5 *Kamerstukken II*, 2015/16, 31 288, nr. 545, p. 5.
6 *Kamerstukken II*, 2015/16, 29 388, nr. 149, p. 5.
7 'Big Data in een vrije en veilige samenleving', WRR-Rapport 95, 2016 en B.H.M. Custers, 'Big Data in wetenschappelijk onderzoek', Justitiële Verkenningen.
8 De zoekterm 'bigdata' geeft op Google 21 miljoen hits.
9 Zie WRR 2016, Zwenne 2015 en Wolters Ruckert & Van Sloten 2016.
10 Zwenne 2015 en Wolters Ruckert & Van Sloten 2016.

data van de zorgverzekeraars en overheid en stellen naar aanleiding van deze casestudy daarbij eveneens principiële vragen over het gebruik van big data.

In deel 3 'Big data en zorginstellingen' onderzoeken mr. Evert-Ben van Veen en mr. Tinga Kleefman het gebruik van big data door de instellingen zelf. Zij genereren niet alleen data, maar verwerken ook big data die zij niet zelf voortbrengen, doch uit hun omgeving betrekken.

Deel 4 'Big data en wetenschappelijk onderzoek' gaat ten slotte over enerzijds 'Big data en open science', door prof. dr. Frank Miedema, en meer algemeen 'Big data, medisch-wetenschappelijk onderzoek en gegevensbescherming' door mr. Menno Mostert.

Aan deze analyses valt te ontlenen dat de ons vertrouwde wereld in rap tempo veranderen zal. Wij zullen ons nieuwe begrippen moeten vormen en juridische categorieën moeten herijken om daar greep op te houden.

Wij wensen u veel plezier bij het lezen van deze preadviezen en zien uit naar een interessant debat over de inhoud ervan op de jaarvergadering.

Prof. mr. Jaap Sijmons
voorzitter Vereniging voor Gezondheidsrecht

INHOUDSOPGAVE

LIJST VAN AFKORTINGEN

AG	advocaat-generaal
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BSN	burgerservicenummer
BW	Burgerlijk Wetboek
CBS	Centraal Bureau voor de Statistiek
CPB	Centraal Planbureau
CTG	College tarieven gezondheidszorg
DBC	diagnose-behandelcombinatie
DIS	DBC-informatiesysteem
DKG	diagnosekostengroep
EHRM	Europees Hof voor de Rechten van de Mens
EPD	elektronisch patiëntendossier
EVRM	Europees Verdrag voor de Rechten van de Mens
EZB	Expertisecentrum Zorgfraudebestrijding
FDEC	Fraude Detectie Expertise Centrum
FKG	farmaciekostengroep
HvJ EU	Hof van Justitie van de Europese Unie
IGZ	Inspectie voor de Gezondheidszorg
KWZi	Kwaliteitswet zorginstellingen
MvT	memorie van toelichting
NAW	naam, adres, woonplaats
NCDR	National Cardiovascular Data Registry
NJ	Nederlandse Jurisprudentie
NTvG	Nederlands Tijdschrift voor Geneeskunde
NZa	Nederlandse Zorgautoriteit
r.o.	rechtsoverweging
RVZ	Raad voor de Volksgezondheid en Zorg
Sr	Wetboek van Strafrecht
Stb.	Staatsblad
Stcrt.	Staatscourant
TvGR	Tijdschrift voor Gezondheidsrecht
UwAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
VWEU	Verdrag betreffende de Werking van de Europese Unie
VWS	Ministerie van Volksgezondheid, Welzijn en Sport
Wbp	Wet bescherming persoonsgegevens
Wet BIG	Wet op de beroepen in de individuele gezondheidszorg
WGBO	Wet op de geneeskundige behandelingsovereenkomst
Wkkgz	Wet kwaliteit, klachten en geschillen zorg
Wmg	Wet marktordening gezondheidszorg
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum

Wtg	Wet tarieven gezondheidszorg
ZIN	Zorginstituut Nederland
Zvw	Zorgverzekeringswet

Deel 1
Gegevenszee en het privacybegrip

1A
Wat is big data?

L. OTTES, ARTS

1B
Big data en privacy. Luctor et emergo?

MR. P.M. KITS

Deel 1
Gegevenszee en het privacybegrip

1A
Wat is big data?

L. Ottes, arts*

* Leo Ottes is senior-adviseur bij de Raad voor Volksgezondheid en Samenleving.

1 Inleiding

Big data staat in het middelpunt van de belangstelling. Volgens (Engelstalige) koppen in kranten en tijdschriften leven we in 'The age of data', 'Big data changes everything' en 'Big data is the next industrial revolution'. In dit inleidende, niet juridische, hoofdstuk wordt nader ingegaan op de vraag: 'Wat is big data eigenlijk?' Zoals zal blijken is er geen eenduidige definitie van dit begrip te geven. Afhankelijk van de invalshoek komt men tot een andere definitie. Drie invalshoeken worden besproken: vanuit de kenmerken van de gegevens, vanuit de techniek, namelijk de opslag en verwerking van gegevens en last but not least vanuit een pragmatische invalshoek: wat is het doel en nut van big data? Het doel van deze bijdrage is de lezer een globaal overzicht te geven over 'het fenomeen' big data. Een aantal technologieën die onlosmakelijk verbonden zijn met big data wordt kort besproken. Met name kan hier gedacht worden aan de sterke opkomst van high-throughput laboratoriumtechnologieën, zoals next generation sequencing en het Internet of Things (IoT). Deze vormen een steeds belangrijker bron van big data. Daarnaast zijn er ontwikkelingen op het terrein van kunstmatige intelligentie in de vorm van kunstmatige neurale netwerken en machine learning. Met name voor dit laatste, zelflerende (computer)systemen, is big data belangrijk.

2 Big data bezien vanuit de kenmerken van de gegevens

Bij big data denkt men direct aan grote hoeveelheden gegevens. Een eerste vraag die rijst is: wat zijn data? Er is evenwel geen juridische definitie van dit begrip. In deze bijdrage worden onder data c.q. gegevens verstaan: feiten en begrippen, weergegeven in een vorm die geschikt is voor het communiceren, interpreteren en verwerken tot informatie, hetzij door de mens, hetzij door machines zoals een computer, dan wel door beide. Gegevens worden informatie als ze betekenis hebben voor de ontvanger. Het interpreteren en integreren van informatie resulteert vervolgens in kennis.

Big data is meer dan alleen een grote hoeveelheid gegevens. Laney beschreef big data in 2001 als een ontwikkeling in drie dimensies met de Engelse termen: *volume*, *velocity* en *variety*: de 3V's.[1] Exponentiële groei van gegevensverzamelingen in alle drie de dimensies tegelijkertijd maakt dat data big data wordt.

1 D. Laney, '3D Data Management: Controlling Data Volume, Velocity, and Variety', Gardner Group, 2001.

2.1 Exponentiële groei van volume

Volume heeft betrekking op de grootte van de gegevensverzameling. In het begin van het computertijdperk werden gegevens in tabelvorm batchgewijs verwerkt. Het ging om gegevensverzamelingen in de grootte van hooguit megabytes (1 MB = 10^6 bytes, waarbij een byte bijvoorbeeld een letter of cijfer kan representeren). Vervolgens kwamen er databases in de orde van grootte van gigabytes (1 GB = 10^9 bytes).
Met de komst van het internet nam de hoeveelheid digitale gegevens sterk toe, van terabytes (1 TB = 10^{12} bytes) naar petabytes (1 PB = 10^{15} bytes). De sensoren van de Large Hadron Collider, waarmee fundamenteel fysisch onderzoek wordt verricht, kan per dag 500 exabytes genereren, meer dan 200 keer zoveel als alle andere gegevensbronnen in de wereld bij elkaar. Slechts een klein deel, 0,001 procent van deze gegevens, kan overigens daadwerkelijk verwerkt worden.[2] Op dit moment wordt er op het internet elke dag circa 1 exabyte (1 EB = 10^{18} bytes) aan gegevens geproduceerd.

Ook binnen de (gezondheids)zorg worden steeds grotere hoeveelheden gegevens geproduceerd en digitaal vastgelegd in onder andere huisartsen- en ziekenhuisinformatiesystemen. Vrijwel alle laboratoriumuitslagen, röntgenfoto's, MRI-, CT- en PET-scans enzovoort, zijn inmiddels gedigitaliseerd. Met name de beeldvormende technieken, zoals (gedigitaliseerde) 'klassieke' röntgenfoto's, MRI's en CT's, genereren veel bytes. In 2011 produceerde het Amerikaans gezondheidssysteem circa 150 exabytes aan gegevens.[3] Ter vergelijking: het totaal aantal woorden dat de mensheid tot op heden heeft uitgesproken wordt geschat op 5 exabytes.[4] De omvang van het elektronische medisch dossier, inclusief röntgenfoto's en dergelijke, van de Californische zorgverlener Kaiser Permanente ligt tussen de 26 en 44 petabytes.[5] Nederlandse ziekenhuizen gezamenlijk genereren per jaar circa 2 petabytes per jaar.[6] Ook in de care is een digitaliseringslag gaande. Gegevens van cliënten worden meer en meer in elektronische cliëntendossiers vastgelegd. De totale omvang is evenwel niet bekend.

---

2 Datascience Central. http://www.datasciencecentral.com/forum/topics/the-3vs-that-define-big-data.

3 P. Cerrato, 'Is Population Health Management the Latest health IT Fad?', *Information Week*, 31 juli 2012.

4 Cerrato, 2012.

5 H.G. Cusack, 'The future state of clinical data capture and documentation: a report from AMIA's 2011 Policy Meeting', *Journal of the American Medical Informatics Association* p. 1-7, 2012.

6 Hekster, big-datadeskundige bij IBM in: 'Big data in de zorg: niet alleen verzamelen', *Medisch Contact* 8 januari 2015, p. 23.

2.2 Toegenomen variëteit van de gegevens

In de begintijd van de computer voerde deze vooral berekeningen uit. Later kwamen er databases waarin allerlei alfanumerieke gegevens werden opgeslagen, zoals namen, adressen van personen, prijzen van producten et cetera. Met behulp van tekstverwerkingsprogramma's kon vrije tekst ingevoerd en opgeslagen worden. Met de komst van de personal computer werd het al snel mogelijk om geluid en foto's te digitaliseren en digitaal te verwerken. Later kwam daar video bij. Tegenwoordig zijn vrijwel alle soorten gegevens, zoals meetwaarden, tekst, geluid, foto's en video, digitaal te genereren of te digitaliseren en op te slaan in standaardformaten, bijvoorbeeld raw, pdf, mp3, jpeg, mp4 etc. Deze kunnen vervolgens digitaal bewerkt en gecommuniceerd worden.

2.3 Toegenomen snelheid van de gegevensverwerking en uitwisseling

Zowel de snelheid van gegevensverwerking als van de uitwisseling van gegevens is de afgelopen decennia exponentieel toegenomen. Door de toename van de verwerkingssnelheid zijn allerlei nieuwe toepassingen binnen handbereik gekomen. Zo zijn er reeds enkele decennia computermodellen beschikbaar om het weer te voorspellen. Echter tot in de jaren negentig van de vorige eeuw duurde het tot wel vijftien dagen om een weersvoorspelling voor de komende zeven dagen door te rekenen. Heden ten dage kan dit in enkele uren, waardoor de modellen praktisch bruikbaar zijn geworden.
Gegevens kunnen ook steeds sneller via het internet uitgewisseld worden, hetgeen ontwikkelingen als streaming video en vlogs mogelijk maakt.

De 3V's moeten in samenhang bezien worden.
Het is de combinatie van toegenomen volume, variëteit en snelheid van verwerking en uitwisseling van digitale gegevens die data tot big data maken. Snelle (draadloze) communicatie van grote hoeveelheden, gevarieerde gegevens, via onder andere mobiele apparaten heeft geheel nieuwe toepassingen mogelijk gemaakt. Zo hebben *social media* in zeer korte tijd een grote impact gekregen op het maatschappelijk leven.

Enkel een grote hoeveelheid gegevens maakt nog geen big data. Zo produceert de Large Hadron Collider uit het eerdere voorbeeld weliswaar een onvoorstelbare hoeveelheid gegevens, in termen van de definitie van de 3V's is het geen big data, omdat variëteit in de data ontbreekt: het gaat enkel om meetwaarden die betrekking hebben op de banen die subatomaire deeltjes afleggen. Een verzameling MRI's in een ziekenhuis kan ook een groot volume hebben, maar ook dit is nog geen big data. Ziekenhuisinformatiesystemen die een grote hoeveelheid patiëntendossiers met een grote variëteit aan gegevens omvatten, komen wel in de buurt, maar zolang het statische databases zijn, waarin gegevens per patiënt vastgelegd worden en bij een consult geraadpleegd, wordt dit nog niet als big

data gezien aangezien de dynamiek van snelle verwerking en uitwisseling ontbreekt. Als er bijvoorbeeld een koppeling wordt gemaakt met ervaringen van patiënten, uitwisseling met het Internet of Things plaatsvindt et cetera, dan gaat het wel richting big data.

Het voorgaande geeft aan dat big data een relatief begrip is. Zoals is aangegeven gaat het om de combinatie van de 3V's, maar er is geen exacte grens aan te geven voor de grootte van de verschillende V's waarboven sprake is van big data. Het is dan ook voor een deel een subjectief begrip. Daar waar de een bij een bepaalde situatie spreekt van big data, vindt de ander dat het gaat om business intelligence of simpelweg om een grote database.

Inmiddels zijn er nog aanvullende 'eisen' bedacht die relevant zijn voor big data. In de traditie van de 3V's worden deze ook met woorden beginnend met een v aangegeven. Zo heeft IBM een vierde V toegevoegd, namelijk *veracity* – waarheidsgetrouwheid.[7] Gegevens van de ene gegevensbron zijn betrouwbaarder dan die afkomstig van een andere. Bij de verwerking moet hiermee rekening worden gehouden. Het Institute for Health Technology Transformation in de VS geeft aan dat met name voor de zorg waarheidsgetrouwheid belangrijk is.[8] Een belangrijke vraag is of gegevens met een lage waarheidsgetrouwheid, zogenoemde *'dirty data'*, getransformeerd kunnen worden in *'clean data'*. Vaak wordt als kracht van big data genoemd dat daarin juist allerlei fouten, onzuiverheden enzovoort zich uitmiddelen, met als resultaat betrouwbare gegevens. Dit is het geval als deze op toeval berusten, maar bij systematische afwijkingen lukt dit echter niet. Systematische afwijkingen zijn evenwel lastig op te sporen.

Andere voorgestelde v's zijn *variability*, waarmee de inconsistentie tussen gegevens wordt bedoeld; *value*, de waarde van de gegevens; *visualisation*, het begrijpelijk presenteren van de gegevens; en tot slot *volatility*, de tijdelijkheid c.q. korte houdbaarheid van de gegevens.[9,10]

2.4 High-troughputtechnieken: het 'omics'-tijdperk

Er is een aantal ontwikkelingen waarbij men niet om het begrip big data heen kan. Een ervan binnen de zorg is de opkomst van zogenoemde high-throughput-laboratoriumtechnieken. Het gaat hier om nieuwe mogelijkheden die ontstaan

7 http://www.ibmbigdatahub.com/infographic/four-vs-big-data.
8 'Transforming Health Care Trough Big Data, Strategies for leveraging big data in the health care industry', Institute for Health Technology Transformation, 2013.
9 Why are the 3 V's not sufficient to describe big data. https://datafloq.com/read/3vs-sufficient-describe-big-data/166.
10 Understanding Big Data: the 7 V's. http://dataconomy.com/seven-vs-big-data/.

door combinaties van technologieën, chemisch, fysisch en ICT. Een voorbeeld is next generation sequencing, waarbij snel en goedkoop het gehele genoom van een individu bepaald kan worden. Er zijn ook high-throughputtechieken ontwikkeld voor het in kaart brengen van al het RNA, het zogenoemde transcriptoom, dat de informatie van het DNA overbrengt naar de eiwitfabriekjes in de cel, de ribosomen, alle eiwitten (proteomics) en voor alle stofwisselingsproducten (metabolomics) in de cel. Daarnaast kan ook het erfelijk materiaal van alle bacteriën die op een bepaalde plaats aanwezig zijn gesequenced worden, waardoor de samenstelling van bacteriepopulaties in en op het lichaam in kaart kan worden gebracht (microbiomics) alsmede in de omgeving. Deze grote hoeveelheden gegevens kunnen gerelateerd worden aan omgevingsfactoren, bijvoorbeeld sociale factoren en aan ziekten en aandoeningen. Dit maakt nieuwe ontwikkelingen mogelijk, zoals de farmacogenetica, waarbij doseringen van geneesmiddelen worden aangepast aan het genetisch profiel van een individuele patiënt.

Privacy is een belangrijk aspect bij medische, meer in het bijzonder genetische, gegevens. Ze hebben specifieke kenmerken. Zo kunnen ze niet geanonimiseerd worden, ze vormen immers de 'genetische vingerafdruk' van een individu. Daarnaast leveren ze niet alleen informatie over het individu, maar ook over zijn of haar bloedverwanten. Binnen de zorg wordt er in het algemeen zorgvuldig met genetische gegevens omgegaan, echter daarbuiten kan men zijn bedenkingen hebben. Zo kan men in het kader van genealogisch onderzoek een aantal genen laten bepalen. Een voorbeeld is de website www.familytreedna.com. Daar worden verschillende DNA-testkits aangeboden om de maternale en/of paternale lijnen na te gaan. Bij de maternale lijn gaat het onder andere om een aantal mitochondriale genen. Mitochondriën worden immers via de moeder doorgegeven. Bij het naspeuren van de paternale lijn gaat het om een aantal genen op het y-chromosoom. Dat kan uiteraard alleen bij mannen. Iedereen kan zo'n test kopen. Op basis van een via de post opgestuurd uitstrijkje van wangslijmvlies worden de genvarianten bepaald. Deze kan men in een database op de site plaatsen en verwanten zoeken. Andere websites, zoals myheritage.com bieden ook tests voor het bepalen van de etnische achtergrond. Er is niet of nauwelijks overheidscontrole of anderszins controle hierop (mogelijk) door het gebrek aan effectieve controlemogelijkheden.

2.5 Internet of Things (IoT)

Bij het Internet of Things, soms vertaald als het 'internet der dingen', gaat het om apparaatjes die, veelal draadloos, verbonden zijn met het internet en autonoom gegevens uitwisselen. De term is reeds in 1999 bedacht door de Engelse ondernemer Kevin Ashton.[11] Een voorbeeld dat vaak wordt genoemd is de koelkast die

11 A. Wood, 'The internet of things is revolutionizing our lives, but standards are a must', *The Guardian*, 31 maart 2015.

zelf de voorraad bijhoudt en automatisch via internet producten bestelt. Het IoT is sterk in opkomst door de combinatie van steeds kleinere en goedkopere sensoren en draadloze communicatietechnieken zoals mobiele communicatie in de vorm van 3G, 4G en in de nabije toekomst 5G, bluetooth en wifi. In producten zoals auto's zitten reeds vele sensoren die de toestand van onder andere de motor monitoren. Op het terrein van gezondheid en zorg gaat het vooral om het monitoren van lichaamsfuncties. Bekend zijn de zogenoemde lifestylegadgets, bijvoorbeeld fitnessarmbanden, horloges en weegschalen, waarmee fysiologische zaken, zoals lichaamsbeweging, slaap(bewegingen) en hartfrequentie gemeten kunnen worden. Daarnaast zijn er draadloze bloeddruk- en zuurstofsaturatiemeters. Er zijn ook reeds apparaatjes op de markt waarmee men zelf ecg's kan maken of urineonderzoeken uit kan voeren. De meetgegevens worden in de regel draadloos doorgegeven aan een smartphone, die de gegevens, eveneens draadloos, via het internet verstuurt. Ook binnen de gezondheidszorg doet het IoT zijn intrede, bijvoorbeeld in de vorm van een pleister die centrale functies zoals temperatuur, hartslag en ecg bewaakt.
Vanuit juridisch perspectief lijkt het in eerste instantie om onschuldige gegevens te gaan, zoals hartslag, waar privacy niet belangrijk lijkt. Echter, recent onderzoek heeft een verband aangetoond tussen hartslag en gewelddadig gedrag.[12] Geweldplegers hebben een gemiddeld lagere hartfrequentie in rust. Als hartfrequenties op grote schaal via het IoT geregistreerd worden, dan zouden met behulp van deze gegevens potentiële criminelen opgespoord kunnen worden.

3 Big data technisch bezien

De exponentiële ontwikkeling van de 3V's uit de vorige alinea wordt mogelijk gemaakt door allerlei technische ontwikkelingen. Zo is de toegenomen snelheid waarmee gegevens verzameld en uitgewisseld kunnen worden, te danken aan zeer snelle en goedkope internetverbindingen, met name glasvezelverbindingen. Ook op het gebied van gegevensopslag zijn er indrukwekkende ontwikkelingen geweest en nog steeds gaande. De opslagcapaciteit is sterk toegenomen terwijl de prijs sterk is gedaald. Zo kostte de opslag van 20 GB aan gegevens in 1980 1 miljoen dollar. De daarvoor benodigde apparatuur besloeg een vijftal archiefkasten en woog 1,5 ton. Tegenwoordig hebben we voor nog geen twintig euro een USB-geheugenstick van 32 GB die slechts enkele tientallen grammen weegt.[13] Hetzelfde geldt voor de verwerkingssnelheid van gegevens. Processoren zijn veel sneller geworden. Deze snelheid loopt nu tegen grenzen aan, maar door meerdere processen gelijktijdig gegevens te laten verwerken – parallel processing – kan de snelheid nog verder opgevoerd worden.[14]

12 A. Latvala et al., 'A longitudinal study of resting heart rate and violent criminality in 700.000 men', *JAMA Psychiatry*;72(10):971-978, september 2015.
13 F. Iafrate, *From Big Data to Smart Data*, ISTE Ltd, 2015, p. 2.
14 Wikipedia. en.wikipedia.org/wiki/Moore%27s_law.

3.1 Non-SQL databases

Naast de ontwikkelingen op het terrein van de hardware zijn er ook ontwikkelingen op het gebied van software. In het verleden gebruikte men voor de opslag van gegevens in de regel relationele-databasemanagementsystemen (RDBMS), ook wel SQL-databases genoemd naar de gebruikte vraagtaal: 'structured query language'. Deze databases zijn zeer betrouwbaar, maar kennen het probleem van schaalbaarheid. Naarmate het volume van de te verwerken gegevens toeneemt, neemt de benodigde tijd ook toe.

Een van de eerste die tegen dit probleem aanliep, was de internetzoekmachine Yahoo!, die in de jaren negentig van de vorige eeuw zeer populair was. Een kernactiviteit van een internetzoekmachine is het indexeren van het internet, ook wel het World Wide Web. Dit groeide in die jaren sterk en het indexeren duurde steeds langer en dreigde vast te lopen. Yahoo! had een computerplatform nodig dat altijd dezelfde hoeveelheid tijd nodig had om het web te indexeren, ongeacht de grootte. Zij ontwikkelde daartoe zelf een computerprogramma, Hadoop genaamd, voor haar tienduizenden dataservers. Dit programma stelde zij vrijelijk als open source beschikbaar.[15] Het programma werd door de internetcommunity in casu de Apache Software Foundation overgenomen. Zij speelt nog steeds een belangrijke rol bij de verdere ontwikkeling. Het Hadoop-platform biedt inmiddels een hele verzameling van opensourcesoftware voor het verwerken van big data.[16] Daarnaast zijn er nog een aantal soortgelijke platforms beschikbaar gekomen.
Hadoop-systemen, combinaties van (standaard)hardware en Hadoop, voor de opslag en verwerking van big data hebben een aantal specifieke kenmerken. Zo worden gegevens niet op één systeem opgeslagen, maar verdeeld over vele dataservers. Het geheel is 'scalable', hetgeen betekent dat het gemakkelijk uitgebreid kan worden tot duizenden servers verdeeld over een of meerdere datacenters.
De servers bestaan uit (relatief) goedkope standaardonderdelen, zoals processoren en harde schijven, tegenwoordig ook steeds meer 'niet-mechanische harde schijven', zogenoemde *solid state drives*, afgekort SSD. Apparaten kunnen defect raken. Bij gebruik van duizenden servers is er altijd wel iets dat hapert. Dit is vaak de mechanische harde schijf waar de gegevens op opgeslagen worden, maar ook SSD's hebben een beperkte levensduur. Dezelfde gegevens worden daarom op meer dan één plek – redundant – opgeslagen, zodat het systeem zichzelf kan herstellen. De gegevens worden door vele servers tegelijkertijd verwerkt op de locatie waar de gegevens worden of zijn opgeslagen: local parallel processing. In de praktijk spreekt men dan ook van 'Hadoop-clusters'. Is er meer opslag- en ver-

15 J. Needham, *Disruptive Possibilities. How Big Data Changes Everything*, Scale Abilities Inc. O'Reilly Media Inc. 2013, p. 4-5.
16 Apache Software Foundation. Hadoop.apache.org.

werkingscapaciteit nodig, dan koppelt men simpelweg extra servers met rekenen opslagcapaciteit aan. Hadoop-clusters kunnen gezien worden als goedkope, schaalbare supercomputers.[17] Door de verkoop van computertijd op Hadoop-clusters zijn supercomputerfaciliteiten inmiddels binnen het bereik van kleinere organisaties en particulieren gekomen.[18] Er zijn inmiddels naast Hadoop ook andere non-SQL-databasesystemen beschikbaar.

3.2 Definitie van big data vanuit technisch perspectief

Gelet op het voorgaande wordt vanuit de technische invalshoek big data wel gedefinieerd als: 'Gegevensverzamelingen die zo groot en complex zijn dat traditionele gegevensverwerkende instrumenten, zoals relationele databases, niet in staat zijn om deze binnen acceptabele tijd en kosten te verwerken.'[19] In deze definitie worden de 3V's in de vorm van 'zo groot en complex' en binnen acceptabele tijd verbonden met het technische aspect.

3.3 De gegevenszee

Zoals hiervoor aangegeven zijn SQL-databases zeer betrouwbaar en ze worden dan ook veel gebruikt, bijvoorbeeld in financiële, ziekenhuis-, huisarts- en apothekerinformatiesystemen. Dit zijn allemaal aparte gegevenssilo's en aan elkaar koppelen is lastig. Een andere mogelijkheid is om de gegevens uit de verschillende bestanden, de gegevenssilo's, te kopiëren naar één groot gegevensbestand om in deze 'zee van gegevens' naar correlaties 'te gaan vissen'. Van der Poel spreekt in dit verband van 'het datameer'.[20] Het woord datameer is evenwel ook de naam van een, op Hadoop gebaseerd, computerprogramma.[21] Om verwarring te voorkomen wordt hier het woord 'gegevenszee' gebruikt.

Vanuit juridisch perspectief is het feit belangrijk dat bij Hadoop- en soortgelijke systemen dezelfde gegevens redundant, dit kan op meerdere plekken in de wereld, zijn opgeslagen, bijvoorbeeld als het gaat om het verwijderen van gegevens. Een ander punt bij non-SQL-databases is dat de data-integriteit minder gegarandeerd is dan bij SQL-databases. Snelheid en schaalbaarheid hebben hun prijs. Data-integriteit is niet alleen bij financiële registratie, maar ook bijvoorbeeld bij patiëntendossiers een must. Dit betekent dat deze gegevens vooralsnog in SQL-databases opgeslagen zullen worden.

---

17 Iafrate, 2015, p. 5.
18 En.wikipedia.org/wiki/Apache_Hadoop. Hadoop Hosting in the Cloud.
19 Big data en privacy. Kamerbrief van de Minister van Economische Zaken, kenmerk DGETM-TM/14179608, 19 november 2014.
20 P. v.d. Poel, 'Duiken in het datameer', *Skipr* 2016;5:11-15.
21 Datameer. www.datameer.com.

4 Big data en een ander manier van denken

Zowel de definitie op basis van de kenmerken van gegevens als die vanuit de technische invalshoek maakt duidelijk dat er verschillend naar big data kan worden gekeken en de grens is vaag tussen wat het wel en wat het niet is. Wat wel in beide definities naar voren komt is dat het steeds een samenkomen van verschillende technologische ontwikkelingen is. Juist deze combinatie zorgt voor nieuwe mogelijkheden om gegevens te genereren, combineren en analyseren. Het biedt mogelijkheden om op een andere manier tegen gegevens aan te kijken, ermee om te gaan en te benutten.

Binnen deze optiek heeft de Nationale DenkTank in haar eindrapport 'Big Data in zicht' uit 2014 als definitie voor big data gekozen: '*Big Data* is de enorme toename van mogelijkheden om data te genereren, combineren en analyseren, die leidt tot nieuwe inzichten en een nieuwe manier van redeneren.'[22]

Daarbij kan een aantal kenmerken onderscheiden worden, zoals de aard van de data, de gebruikte gegevensbronnen, de gehanteerde analysetechnieken en het gebruik van de resultaten.

Aard van de data: Er is sprake van grote hoeveelheden zeer gevarieerde gegevens waaronder veel die vaak on- of semigestructureerd zijn (volume en variety).

Gegevensbronnen: Gegevens afkomstig van verschillende gegevensbronnen, die zich veelal in verschillende domeinen bevinden, worden gecombineerd. Dit leidt tot ontschotting van domeinen: gegevens uit het ene domein worden gebruikt voor beslissingen in het andere domein.

Analysetechnieken: De analysetechnieken zijn *data-driven*. Dit betekent dat naar patronen gezocht wordt zonder dat vooraf hypothesen zijn opgesteld zoals bij de klassieke aanpak. De resultaten zijn snel beschikbaar en geven daardoor inzicht in het nu: *(near) realtime* c.q. *nowcasting*. Ze kunnen voorspellende waarde hebben: *predictive analysis/forecasting*.

Gebruik: De resultaten op geaggregeerd niveau kunnen toegepast worden op beslissingen op groeps- of individueel niveau.

Vanuit een juridische invalshoek is met name het feit relevant dat gegevens afkomstig zijn uit verschillende gegevensbronnen, die zich vaak ook nog in verschillende domeinen bevinden. Het gaat om het koppelen van gegevensbestan-

22 'Big Data in zicht. 10 oplossingen voor maatschappelijke impact met Big Data', Eindrapport 2014. Stichting de Nationale Denktank, www.nationale-denktank.nl/eindrapport2014.

den waarbij gezocht wordt naar patronen die vooraf niet bekend zijn. Dit kan op gespannen voet staan met zaken als de bescherming van de persoonlijke levenssfeer, doelbindingsvereiste bij het registeren van gegevens en informed consent. Het gaat veelal om de afweging van het belang van het individu versus het belang van de samenleving als geheel. Het is daarom belangrijk om te bezien welke potentiële bijdrage big data kan leveren aan het algemeen belang. Op het terrein van de zorg is dit bijvoorbeeld bijdragen aan de wetenschappelijke kennis om gezondheid te bevorderen en ziekten en aandoeningen beter te kunnen diagnosticeren en behandelen, het verhogen van de effectiviteit en doelmatigheid van de zorgverlening door betere sturings- en managementinformatie, et cetera.

5 Voorbeelden van big data in de zorg

Zoals in de vorige paragraaf is aangegeven kan (het gebruik van) big data op gespannen voet staan met het belang van het individu. Een belangrijke vraag is dan ook wat big data kan bijdragen aan het algemeen belang en aan het belang van het individu. Aan de hand van een aantal voorbeelden wordt het nut van big data voor de zorg geschetst.

5.1 Onderzoek naar de relatie tussen ziekte en omgevingsfactoren

Onderzoek naar de relatie tussen ziekte en omgevingsfactoren kent een lange historie en heeft in het verleden een grote bijdrage geleverd aan de volksgezondheid. Het gaat hierbij om het ontdekken van verbanden: systematisch analyseren van gegevens en het bij elkaar brengen van allerlei puzzelstukjes. Klassiek is de ontdekking van Snow dat de cholera-epidemie in 1845 in Londen werd veroorzaakt door besmet water uit een waterpomp op Broadstreet door het verspreidingspatroon van de ziekte in kaart te brengen. De infectietheorie bestond in die tijd nog niet. De algemene theorie was dat cholera veroorzaakt werd door slechte lucht. Door zorgvuldige statistische analyse van de locatie van choleragevallen kon hij het verband tussen de kwaliteit van het bronwater en cholera aantonen. Bij epidemiologische studies worden de principes van Snow nog steeds toegepast, maar nu wordt ook big data ingezet.[23] Zoals in de vorige paragraaf is aangegeven gaat het bij big data juist om het vinden van verbanden tussen gegevens afkomstig van verschillende gegevensbronnen.

5.2 Opsporen van bacteriën in de New Yorkse metro

Een voorbeeld van modern epidemiologisch onderzoek gebaseerd op big data is het opsporen van bacteriën in de New Yorkse metro. Onderzoekers van het Weill Cornell Medical College in New York verzamelen in een lopend onderzoek bacte-

23 nl.wikipedia.org/wike/John_Snow.

riesamples van bijvoorbeeld handvatten en deurknoppen, tourniquets en kaartjesautomaten in de 466 metrostations en treinstellen in verschillende delen van New York. Het DNA in de samples wordt gesequenced. De 10 miljard fragmenten worden door een supercomputer gesorteerd en vergeleken met een database van bekende bacteriën. De resultaten van dit *PathoMap*-project laten veel 'problematische' bacteriën zien. Zo blijkt dat in bijna de helft van de stations antibioticaresistente bacteriën en bacteriën die voedselvergiftiging kunnen veroorzaken, voorkomen. Minder frequent komen veroorzakers van hersenvliesontsteking voor. Zelfs de bacterie die builenpest veroorzaakt is gevonden. Het bleek ook dat er verschillende bacteriepopulaties in verschillende wijken van New York voorkomen. Een belangrijke vraag is welke relatie dit heeft met bijvoorbeeld verschillende ziektepatronen in verschillende wijken.[24]

5.3 Opsporen van bijwerkingen van geneesmiddelen

Voordat een geneesmiddel op de markt mag worden gebracht moet het uitgebreid getest worden in zogenoemde *clinical trials*. Als de beoordelingsautoriteit het middel veilig en werkzaam acht, laat zij het toe tot de markt. Echter, nadat het middel op de markt is gekomen en aan een brede patiëntenpopulatie wordt voorgeschreven, kunnen zeldzame bijwerkingen optreden die niet eerder zijn opgemerkt. Big data kan een belangrijke rol spelen bij de ontdekking hiervan. Een voorbeeld hiervan is de vaststelling van een gevaarlijke bijwerking van het geneesmiddel Vioxx. Dit kwam in 1999 op de markt. Het middel werd vooral voorgeschreven aan patiënten met reumatoïde artritis. Al snel ontstonden er verdenkingen dat het middel als bijwerking een hartinfarct of plotse hartdood kon geven. Zorgverlener Kaiser Permanente analyseerde de gegevens van 1,4 miljoen verzekerden en kon de gevaarlijke bijwerkingen cijfermatig onderbouwen. Mede op basis van deze informatie werd het middel in 2004 van de markt gehaald.[25]

5.4 Voedselveiligheid controleren met hulp van big data

Onhygiënische toestanden in restaurants leiden regelmatig tot voedselvergiftigingen. De overheid heeft daarom hygiënerichtlijnen opgesteld. Inspecteurs controleren de naleving daarvan. In Chicago gebeurt dat door 32 voedselinspecteurs – *sanitarians* – die de 15.000 restaurants in de stad moeten controleren. Zij kunnen niet alle restaurants bezoeken en selecteren dan ook de meest risicovolle. Dit gebeurt op klassieke wijze, op basis van risicofactoren. Deze factoren zijn opgesteld na analyse van gedurende zo'n tien jaar verzamelde gegevens. Gegevens zoals eerdere overtredingen en de locatie van het restaurant bleken minder van belang dan bijvoorbeeld het voorkomen van weersituaties waarbij ingrediënten

24 R.L. Hotz, 'Big Data and Bacteria: Mapping the New York Subway's DNA', *The Wall Street Journal*, 5 februari 2015.

25 http://www.fda.gov/NewsEvents/Testimony/ucm113235.htm.

sneller bederven. Tot voor kort waren de controleurs voor het registreren van voedselvergiftigingen vooral aangewezen op meldingen van restaurants zelf. Gebleken is dat mensen op sociale media melden als zij misselijk zijn en moesten braken. Er is een computerprogramma ontwikkeld dat Twitterberichten scant op woorden die gelinkt kunnen zijn met restaurantbezoek en voedselvergiftiging, zoals braken, overgeven, enzovoort. Degenen die een dergelijk bericht versturen, wordt gevraagd om informatie en verzocht hun ervaringen te rapporteren aan de inspectie.[26]

New York maakt gebruik van het sociale netwerk Yelp[27]. Op deze site kunnen mensen beoordelingen plaatsen van winkels, restaurants of producten. Het New York Department of Health and Mental Hygiene (DOHMH) analyseert de *crowdsourced reviews* over restaurants. Net als in Chicago scant een computerprogramma de berichten op woorden die gelinkt kunnen zijn met voedselvergiftiging. Deze worden nader onderzocht. Uit een analyse gedurende negen maanden, waarbij 294.000 reviews werden gescreend, bleek dat er drie uitbraken waren gevonden die niet via de officiële kanalen waren gemeld.[28]

Volgens een bericht in de *Washington Post* maakt men in New York inmiddels ook gebruik van Twitterberichten. Berichten die een indicatie kunnen geven van een mogelijke voedselvergiftiging tracht men te koppelen aan mogelijke berichten van dezelfde twitteraar enkele dagen daarvoor waarin deze melding maakt van een restaurantbezoek. Clustering van meerdere meldingen kunnen de inspecteurs naar een specifiek restaurant leiden.[29]

5.5 Verbeteren van de kwaliteit en doelmatigheid van de zorg met behulp van big data

Met name in de Verenigde Staten wordt big data ingezet voor kostenreductie. In het tijdschrift *Health Affairs* is een aantal onderzoeksresultaten gepubliceerd.[30] Zo onderzochten Bates et al. het management van patiënten met hoge zorgkosten. Vijf procent van de patiënten is verantwoordelijk voor de helft van de zorgkosten in de Verenigde Staten. Het is belangrijk deze te identificeren c.q. te voorspellen wie dit zijn, zodat zorgverleners tijdig kunnen behandelen.
Voorbeelden van enkele projecten zijn de volgende.

---

26 J.K. Harris, 'Health Department Use of Social Media to Identify Foodborne Illness – Chicago, Illinois, 2013-2014', Centers for Disease Control and Prevention, Morbidity and Mortality Weekly Report August 15, 2014 / 63(32);681-685.

27 www.yelp.com en www.yelp.nl.

28 C. Harrison et al., 'Using Online Reviews by Restaurant Patrons to Identify Unreported Cases of Foodborne Illness – New York City, 2012-2013', Centers for Disease Control and Prevention, May 23, 2014 / 63(20);441-445.

29 M. Ravindanath, 'In Chicago, food inspectors are guided by big data', *The Washington Post*, 28 september 2014.

30 Health Affairs, 8 juli 2014.

Project Artemis
Binnen het project Artemis, ontwikkeld door het Institute of Technology van de Universiteit van Ontario, Canada, wordt de grote datastroom die het monitoren van pasgeborenen op de intensive care genereert, continu geanalyseerd. Ziekenhuisinfecties kunnen daardoor 24 uur voordat zich symptomen openbaren voorspeld worden. Daardoor kan een behandeling eerder gestart worden, waardoor de overlevingskansen van pasgeborenen toenemen.[31]

Data mining voor optimalisatie van knieoperaties en bloedtransfusies
Orthopedisch chirurgen in het Brigham and Women's Hospital in Boston analyseerden grote hoeveelheden patiëntgegevens en isoleerden de factoren die bepalend zijn voor het succes van knieoperaties. Door het systematisch standaardiseren van de operaties nam de succeskans toe en namen de kosten af. Op eenzelfde wijze wist de Universiteit van Michigan de noodzaak voor toediening van bloedtransfusies met 31 procent te verminderen. Behalve in een vermindering van risico's voor de patiënt, resulteerde het in een kostenbesparing van 200.000 dollar per maand.[32]

Big data voor de selectie van risicovolle zorgverleners
De Inspectie voor de Gezondheidszorg (IGZ) maakt inmiddels ook gebruik van big data voor het selecteren van risicovolle zorgverleners. Voor dit zogenoemde risicogestuurd toezicht heeft de IGZ een dashboard ontwikkeld. Het is een instrument om inspecteurs te helpen om risico's in de zorg te detecteren. Het dashboard bestaat uit een computerprogramma waarmee op een overzichtelijke en compacte wijze informatie wordt getoond die gerelateerd is aan kwaliteit en veiligheid van zorg. Veel van deze informatie is afkomstig van registraties waaraan instellingen gegevens leveren, zoals Dutch Hospital Data[33]. Daarnaast zijn er nog andere bronnen zoals jaarverslagen. Trends in relevante gegevens, zoals ziekenhuissterfte, worden getoond. Al deze informatie vormt input voor het prioriteren en inrichten van het toezicht. In 2014 vond in samenwerking met de Radboud Universiteit een onderzoek plaats naar de mogelijkheid van het gebruik van sociale media. Immers, op sociale media beschrijven patiënten regelmatig hun ervaringen met de zorg. Een belangrijke website in dit kader is zorgkaartnederland.nl van de patiëntenfederatie NPCF. Op deze site staan veel beoordelingen van zorgaanbieders door patiënten. De patiëntervaringen zijn inmiddels geïntegreerd in het dashboard voor risicogestuurd toezicht.

31 Artemis Project. University of Ontario (http://hir.uoit.ca/cms/?q=node/24).
32 Healthcare IT News, 12 juni 2012.
33 Dutch Hospital Data. www.dhd.nl.

6 Big data en kunstmatige intelligentie

Reeds vanaf de jaren zestig van de vorige eeuw poogt men kennis van deskundigen 'af te tappen' en in een computer te brengen. Dit is het terrein van de kunstmatige intelligentie. Een van de eerste programma's op het terrein van de geneeskunde was MYCIN. Het programma was gericht op het diagnosticeren en behandelen van bacteriële infecties met antibiotica en kon in 69 procent van de gevallen de juiste therapie selecteren.[34] Nu lijkt dit percentage niet zo hoog, doch het programma deed het beter dan de gemiddelde arts. Ondanks dat MYCIN het beter deed, is het systeem nooit in de dagelijkse praktijk gebruikt. De belangrijkste reden was dat de technologie er nog niet klaar voor was. In de jaren zeventig bestond de personal computer nog niet. De gebruiker moest de antwoorden op de vragen die MYCIN stelde intypen, waarna het programma op een *time-shared* systeem ruim een half uur nodig had om tot een antwoord te komen.

Tegenwoordig zijn deze technologische problemen grotendeels opgelost. Toch zijn rule-based expertsystemen zoals MYCIN nooit echt doorgebroken in de dagelijkse praktijk. Het grote probleem bij de ontwikkeling bleek het aftappen van de kennis van de expert, de zogenoemde kennisacquisitie-bottleneck. De kennis moet opgeslagen worden in een kennisbestand in de vorm van besluitvormingsregels. Het kennisbestand van MYCIN bestond uit circa 600 regels.[35] Het blijkt heel moeilijk om de kennis van experts om te zetten in besluitvormingsregels.

De kennisacquisitie-bottleneck kan opgelost worden met big data. De computer kan met big data 'gevoed' worden en hier kennis uit genereren ('machine learning'). Verschillende bedrijven zijn actief op dit terrein, waaronder IBM en DeepMind, een zusterbedrijf van Google. Deze vorm van kunstmatige intelligentie wordt, op experimentele basis, reeds in de zorgpraktijk toegepast. Een voorbeeld hiervan is beschreven in een artikel in *The Japan Times*.[36] Een patiënte in een universiteitsziekenhuis in Tokyo reageerde niet goed op een maanden durende chemotherapie voor acute myeloïde leukemie. Het vermoeden rees dat er sprake was van een ander type leukemie, maar dat kon met gangbare testen niet aangetoond worden. Haar genetische informatie werd ingevoerd in Watson, de supercomputer van IBM. Een zoektocht door zijn database met oncologiegegevens leverde als diagnose op dat ze een zeldzame vorm van secundaire leukemie had. De patiënte reageerde vervolgens goed op een aangepaste therapie.

---

34 B.G. Buchanan, E.H. Shortliffe, *Rule-Based Expert Systems The Mycin Experiments of the Stanford Heuristic Programming Project*, Addicon Wesley 1984.

35 en.wikipedia.org/wiki/Mycin.

36 T. Otake, 'IBM big data used for rapid diagnosis of rare leukemia case in Japan', *The Japan Times*, 11 augustus 2016.

6.1 Aansprakelijkheid

Een belangrijk probleem bij het stellen van een diagnose door de computer is de juridische aansprakelijkheid. De arts is immers eindverantwoordelijk. Een ander punt is of een computerdiagnose ook daadwerkelijk geaccepteerd wordt. Als uit wetenschappelijk onderzoek zou blijken dat de computer beter diagnosen kan stellen, willen we er dan op vertrouwen?

6.2 Privacy

Een ander probleem is de privacy van patiënten. De computer moet immers grootschalige toegang hebben tot onder andere patiëntgegevens om hier nuttige kennis uit te halen. In het Verenigd Koninkrijk ontstond in mei 2016 grote opschudding toen bleek dat de NHS, de national health service, aan DeepMind toegang had gegeven tot de medische dossiers van ongeveer 1,6 miljoen patiënten in drie ziekenhuizen. Het bedrijf kreeg daarbij toegang tot niet-geanonimiseerde gegevens.

In het big-datatijdperk wordt het overigens steeds lastiger om gegevens echt te anonimiseren. Door het combineren van gegevens uit diverse bronnen is de kans groot dat gegevens gedeanonimiseerd kunnen worden.[37] Zo bleek 40 procent van de anonieme deelnemers aan een DNA-onderzoek via geavanceerde analyses toch geïdentificeerd te kunnen worden.[38] Degenen die stellen: 'Privacy is a thing of the past' lijken het gelijk aan hun zijde te hebben.[39] Burgers zeggen weliswaar zich zorgen te maken over hun privacy, maar in hun gedrag blijkt hier weinig van, gezien het gemak waarmee ze allerlei gegevens via sociale media openbaar maken. Op internet betaalt de gebruiker voor veel 'gratis' diensten met zijn privacy. Privacy lijkt te verschuiven van iets waarop men recht heeft, naar iets waarvoor men moet betalen. De vraag is of dit ook voor zorggegevens gaat gelden.

6.3 Wie is eigenaar van computergegenereerde kennis?

In een aantal gevallen kan er voor de kennisacquisitie gebruikgemaakt worden van geanonimiseerde gegevens. Een recent voorbeeld van dit laatste is DeepMind die met het Moorfields Eye Hospital in het Verenigd Koninkrijk een partnership is aangegaan. Een miljoen (geanonimiseerde) oogscans, naast netvliesfoto's ook zogeheten *optical coherence tomography scans*, zullen de komende vijf jaar geanaly-

37 P. Ohm, 'Broken promises of privacy: responding to the surprising failure of anonymization', *UCLA Law Rev*. 2010;57;1701-77.

38 A. Tanner, 'Harvard professor reidentifies anonymous volunteers in DNA study', *Forbes* 25 april 2013.

39 Why privacy is a thing of the past. http://www.theguardian.com/technology/2013/oct/06/big-data-predictive-analytics-privacy.

seerd worden. De kennis die daardoor gegenereerd wordt en deel uitmaakt van de te ontwikkelen AI-software, wordt eigendom van het bedrijf.
Binnen de wetenschappelijke wereld wordt de opvatting breed gedragen dat informatie en daaruit verkregen kennis vrijelijk beschikbaar moet zijn voor iedereen. Het is evenwel niet ondenkbaar dat er, net als bij de internetzoekmachines en sociale media, natuurlijke monopolies ontstaan, waarbij een of enkele dominante partijen de kennis extraheren uit vrijelijk beschikbare wetenschappelijke gegevens. Deze kennis is hun eigendom en zoals Francis Bacon reeds zei: 'Ipsa scientia potenta est' (kennis zelf is macht).

7 Nieuwe juridische kaders nodig

In het voorgaande is een globaal overzicht gegeven van big data. Een drietal invalshoeken is verkend: de kenmerken van de gegevens, de technische invalshoek en de invalshoek van het gebruik van big data die een andere manier van denken mogelijk maakt, namelijk niet hypothesegericht maar data-driven, waarbij men op zoek gaat naar onvoorziene correlaties in grote verzamelingen aan zeer gevarieerde en uit verschillende bronnen verkregen gegevens, de gegevenszee. Big data vormt daarnaast het 'voedsel' voor zelflerende systemen die op basis van kunstmatige intelligentie kennis produceren.

Nieuwe ontwikkelingen leiden tot nieuwe juridische vragen. Wetgeving loopt altijd achter op deze ontwikkelingen. Zo was de Wet persoonsregistraties van 1989, met een 'upgrade' in 2001 met de Wet bescherming persoonsgegevens, een gevolg van het ontstaan van een groot aantal gegevensbestanden met persoonsgegevens dat mogelijk was geworden door de komst van (kleinere) geautomatiseerde informatiesystemen, met name de personal computer.

Inmiddels leven we in het (draadloze) internet-, IoT-, 'omics-' en big-datatijdperk. Kunstmatige intelligentie, waarbij de gegevenszee geautomatiseerd, zonder tussenkomst van de mens, wordt geanalyseerd, zal meer en meer ingang vinden.

Big data is een ontwikkeling die grote gevolgen heeft voor zowel de samenleving als het individu. Het biedt kansen, maar levert ook gevaren op. Een belangrijke juridische vraag is hoe fundamentele mensenrechten in het big-datatijdperk geborgd kunnen worden.

Literatuur

Buchanan, Shortliffe (1984)
B.G. Buchanan, E.H. Shortliffe, *Rule-Based Expert Systems The Mycin Experiments of the Stanford Heuristic Programming Project*, Addicon Wesley 1984.

Cerrato (2012)
P. Cerrato, 'Is Population Health Management the Latest health IT Fad?', *Information Week*, 31 juli 2012.

Cusack (2012)
H.G. Cusack, 'The future state of clinical data capture and documentation: a report from AMIA's 2011 Policy Meeting', *Journal of the American Medical Informatics Association* p. 1-7, 2012.

Harris (2014)
J.K. Harris, 'Health Department Use of Social Media to Identify Foodborne Illness – Chicago, Illinois, 2013-2014', Centers for Disease Control and Prevention, Morbidity and Mortality Weekly Report August 15, 2014 / 63(32);681-685.

Harrison et al. (2014)
C. Harrison et al., 'Using Online Reviews by Restaurant Patrons to Identify Unreported Cases of Foodborne Illness – New York City, 2012-2013', Centers for Disease Control and Prevention, May 23, 2014 / 63(20);441-445.

Hotz (2015)
R.L. Hotz, 'Big Data and Bacteria: Mapping the New York Subway's DNA', *The Wall Street Journal*, 5 februari 2015.

Iafrate (2015)
F. Iafrate, *From Big Data to Smart Data*, ISTE Ltd, 2015.

Institute for Health Technology Transformation (2013)
'Transforming Health Care Trough Big Data, Strategies for leveraging big data in the health care industry', Institute for Health Technology Transformation, 2013.

Laney (2001)
D. Laney, '3D Data Management: Controlling Data Volume, Velocity, and Variety', Gardner Group, 2001.

Latvala et al. (2015)
A. Latvala et al., 'A longitudinal study of resting heart rate and violent criminality in 700.000 men', *JAMA Psychiatry*;72(10):971-978, september 2015.

Needham (2013)
J. Needham, *Disruptive Possibilities. How Big Data Changes Everything*, Scale Abilities Inc. O'Reilly Media Inc. 2013.

Ohm (2010)
P. Ohm, 'Broken promises of privacy: responding to the surprising failure of anonymization', *UCLA Law Rev.* 2010;57;1701-77.

Otake (2016)
T. Otake, 'IBM big data used for rapid diagnosis of rare leukemia case in Japan', *The Japan Times*, 11 augustus 2016.

Poel (2016)
P. v.d. Poel, 'Duiken in het datameer', *Skipr* 2016;5:11-15.

Ravindanath (2014)
M. Ravindanath, 'In Chicago, food inspectors are guided by big data', *The Washington Post*, 28 september 2014.

Stichting de Nationale Denktank (2014)
'Big Data in zicht. 10 oplossingen voor maatschappelijke impact met Big Data', Eindrapport 2014. Stichting de Nationale Denktank, www.nationale-denktank.nl/eindrapport2014.

Tanner (2013)
A. Tanner, 'Harvard professor reidentifies anonymous volunteers in DNA study', *Forbes* 25 april 2013.

Wood (2015)
A. Wood, 'The internet of things is revolutionizing our lives, but standards are a must', *The Guardian*, 31 maart 2015.

Deel 1
Gegevenszee en het privacybegrip

1B
Big data en privacy. Luctor et emergo?

Mr. P.M. Kits

* Peter Kits is partner IP/IT & Privacy bij Deloitte Legal te Amsterdam.

Luctor et emergo?
'De opgave, aan het recht gesteld, lijkt op die van de geneeskunde. Soms gaat het wonderlijk lang goed, maar op den duur bereiken beide de grens waar ze niet overheen kunnen. De dood is voor de medicus wat het onrecht is voor de rechter: onontkoombaar, maar daarom fel en voortdurend bestreden' – Jan Leijten, uit: *De achterkant van het recht*, 1994.

1 Inleiding

Big data zal volgens velen een revolutie veroorzaken in de manier waarop we leven, werken en denken. Door de digitalisering zijn de mogelijkheden voor toegang tot, uitwisseling, gebruik én hergebruik van gegevens, technologisch gezien, vrijwel onbegrensd en zijn zelflerende computers ontwikkeld.[1] Door deze technologische ontwikkelingen zijn bigdatatoepassingen mogelijk geworden. Beslissingen zullen dan ook steeds vaker, in de toekomst wellicht zelfs uitsluitend, genomen worden op basis van bigdata-analyses door computers in plaats van op basis van intuïtie door de mens. Deze ontwikkeling verloopt mede razendsnel (lees: exponentieel) doordat dagelijks miljarden computertransacties via internet door gebruikers (de mens zelf) worden uitgevoerd.[2]

Bij big data gaat het om het inzichtelijk worden van onverwachte connecties en relaties (correlaties). Dit gebeurt door analyse van meestal grootschalige en diverse gekoppelde databestanden. Deze analyse gebeurt door algoritmes. Dit zijn in computertaal geprogrammeerde wiskundige formules die bepalen welke stappen de computer moet doorlopen, bijvoorbeeld via regels: 'als x dan y'.[3]

Ten behoeve van betere duiding is van belang te realiseren dat big data niet hetzelfde is als *business intelligence* of traditionele *data analytics*. Bij deze twee gaat het om het zoeken naar antwoorden op vragen van bijvoorbeeld de oorzaak van bepaald gedrag of naar een bepaalde gewenste uitkomst, door 'bekende' en logische informatie- en databestanden te analyseren. In die gevallen weet men waar men naar zoekt. Bij big data gaat het om nog onbekende correlaties en door algoritmes bepaalde uitkomsten (en daarop gebaseerde beslissingen).

---

1 Zoals de bekende Watson (IBM) en Siri (Apple).

2 De essentie van de veranderingskracht van nieuwe digitale technologieën is, dat, veelal onbewuste, economische *trade offs* maken tot wie we zijn en wat we doen. Kort gezegd: we gebruiken WhatsApp, Facebook en Google en 'betalen' met onze privégegevens doordat onze voorkeuren en gedrag gedeeld wordt met bedrijven die gepersonaliseerde advertenties sturen of aanbiedingen doen. Hierdoor neemt het gebruik verder toe en worden de computers steeds slimmer. Zie: L. Moerel, *Big Data Protection, How to make the Draft EU Regulation Data Protection Future Proof*, Tilburg University, 2014, p. 3.

3 Over de macht van algoritmes zie par. 6.2.

Big data in de zorg staat op het punt een grote doorbraak te maken. Recent ontving UMC Utrecht een bedrag van 20 miljoen euro van het Europese Innovative Medicine Initiative voor onderzoek naar de inzet van big data: Bigdata@heart. Data uit de dagelijkse zorg, geanonimiseerd of met toestemming van de patiënt, zal worden samengevoegd met data uit studies en data afkomstig van zogenoemde wearables.[4]

Twee belangrijke initiatieven die de vloer voor big data in de zorg effenen zijn: 'Parelsnoer' en 'Registratie aan de bron'. Het Parelsnoer Instituut (een samenwerkingsverband van de Universitaire Medische Centra in Nederland) heeft als missie integratie van zorg en wetenschap te behouden en uit te breiden in elk UMC, op het hoogst mogelijke kwaliteitsniveau, door standaardisatie en harmonisatie van het zorgproces, met verzameling van data, beelden en lichaamsmaterialen die beschikbaar zijn en blijven voor wetenschappelijk onderzoek.[5] 'Registratie aan de bron', een initiatief van de Nederlandse Federatie van Universitair medische centra (NFU) en Nictiz, wil ervoor zorgen dat alle zorginformatie eenduidig en eenmalig wordt geregistreerd. 'Alleen dan is die informatie voor zo veel mogelijk doeleinden te hergebruiken'.[6]

Big data in het kader van de zorg zal een grote impact hebben op de privacy, het recht op gegevensbescherming en het, daarmee onlosmakelijk verbonden, beroepsgeheim.
Decennialang was het basisprincipe van privacywetgeving, overal ter wereld, burgers zelf te laten bepalen of, hoe en door wie hun persoonlijke informatie mag worden verwerkt.[7] Echter nu in het internettijdperk is dat 'zelfbeschikkingsrecht'

4 www.skipr.nl/actueel/id28685-umc-utrecht-krijgt-20-miljoen-voor-big-data-onderzoek.html.

5 Parelsnoer biedt onderzoekers binnen de UMC's én externe onderzoekers een infrastructuur en geactualiseerde standaardprocedures voor het opzetten, uitbreiden en optimaliseren van klinische biobanken ten behoeve van wetenschappelijk onderzoek. http://parelsnoer.org/page/nl/Home.

6 www.registratieaandebron.nl.

7 In 1980 publiceerde de OECD (Organisation for Economic Co-operation and Development) 'Guidelines on the Protection of Privacy and Transborder Flows of Personal data'. Hierbij was de doelstelling om fundamentele, maar concurrerende, waarden, zoals privacy en het recht op vrije toegang tot informatie, in balans te brengen door minimumstandaarden voor gegevensbescherming voor persoonsgegevens vast te stellen. Daarbij staat het individu centraal: 'Their central requirement is that the collection and use of personal data be both limited and lawful – that is, either explicitly permitted by law or consented to by individuals to whom the data pertains […]'. In: *Data Protection Principles for the 21st Century, revising the OECD Guideline*, Fred H. Cate, P. Cullen, V. Mayer-Schonberger, 2013, p. 5.

verworden tot een statisch administratief systeem van 'informeren en toestemming vragen', waarbij van een doeltreffende en adequate bescherming van de privacy niet meer kan worden gesproken. In het bigdatatijdperk, waarin de waarde van de gegevens juist is gelegen in het hergebruiken van data voor toepassingen die bij het verzamelen van de data vaak niet werden voorzien, is zo'n systeem zelfs expliciet ongeschikt voor het garanderen van de privacy en borging van het beroepsgeheim.[8]

In dit deel van het preadvies gaat het om het recht op privacy in het licht van big data in de zorg. Hierbij ga ik in op de volgende vragen:
- Wat zijn de kansen en risico's van big data in de zorg? (2)
- Wat is data? Waar komen de data vandaan? (3)
- Wat zijn de bronnen van data? (4)
- Wat is het juridisch kader? Wat houdt het privacy begrip in het licht van big data (nog) in? (5)
- Wat zijn knelpunten? (6)
- En tot slot, hoe zouden de knelpunten opgelost en de grondrechten van het individu en in het zorgproces de patiënt, effectief kunnen worden beschermd in het bigdatatijdperk? (7)

2 Wat zijn de kansen en risico's van big data in de zorg?

Als kansen van big data in de zorg worden algemeen beschouwd: data-analyses die informatie verschaffen ten behoeve van:
- effectievere en betere behandeling van de patiënt in en voorafgaand aan het zorgproces (curatief);
- effectievere en betere preventie van ziekten en aandoeningen;
- efficiencyslagen/kostenbesparing[9];
- kwaliteitscontroles[10];
- (biomedisch) wetenschappelijk onderzoek en *clinical trials;*
- beleidsdoeleinden.

Als voornaamste risico's worden wel genoemd:
- doorbreking van het beroepsgeheim;
- verlies en/of verminking van gevoelige (persoons)gegevens;
- toegang of gebruik door onbevoegden van die gegevens; en/of

8 V. Mayer-Schönberger en K. Cukier, *De Big Data Revolutie*, Maven Publishing, 2013, p. 242.

9 In 2014 bedroegen de zorgkosten in Nederland maar liefst 95 miljard euro, oftewel ruim € 5.630 per hoofd van de bevolking. Bron: CBS.

10 Zie: https://www.dica.nl/ (cure) en https://www.sbggz.nl/ (ggz).

– inbreuken op de persoonlijke levenssfeer van de patiënt of burger bijvoorbeeld door profiling[11];
– ongecontroleerde handel in medische data en misbruik van data voor commerciële doelen, zoals het mogelijk weigeren van burgers of groepen personen voor verzekeringen of zorg, door informatie verkregen uit data-analyses via (gekoppelde) databestanden.

3 Wat is data en wie behoren ze toe?

Data of gegevens (deze woorden zullen in het navolgende door elkaar worden gebruikt, maar hebben steeds dezelfde betekenis) betreffen in feite leesbare of verwerkbare 'waarden', zoals woorden en cijfers.[12] Deze data bevinden zich op harde schijven en in data- en/of biobanken die het mogelijk maken bruikbare of waardevolle gegevensverzamelingen te creëren of er informatie[13] van te maken. Dit gebeurt door de data te analyseren, te koppelen aan of samen te voegen met andere data of ze in een bepaalde context te plaatsen. Voor big data zijn 'ruwe data', dat wil zeggen onbewerkte data, de grondstof. Veel data is op dit moment nog niet 'ruw' genoeg, doordat deze zijn opgeslagen in bestandsformaten die niet bewerkbaar zijn, zoals pdf. Initiatieven zoals 'Parelsnoer' en 'Registratie aan de bron' werken aan oplossingen voor een betere 'ontsluitbaarheid' van zorgdata.

Volgens het Nederlands recht komen data *sec* niet in aanmerking voor eigendom in de zin van het vermogensgoederenrecht. Data betreffen noch een zaak (art. 3:2 BW) noch een vermogensrecht (art. 3:6 BW). Het onderwerp eigendom van medische data is enkele malen in de rechtspraak naar voren gekomen. In 1981 wees het Hof Den Haag een vordering tot afgifte van röntgenfoto's aan de patiënt op grond van eigendom af.[14] Volgens het Hof Den Bosch komt het origineel van een ziektegeschiedenis toe aan de opsteller of degene die het heeft doen opstellen.[15]

---

11 Profiling heeft als doel het totaal volgen van complete populaties of doelgroepen om middels in te stellen criteria en normen '*outliers*' te identificeren. Outliers zijn afwijkingen van de norm, mensen die ander gedrag vertonen dan de 'normaalgroep', of een specifieke groep die de interesse heeft van de overheid of het bedrijfsleven. Bron: http://webwereld.nl/big-data/59982-profiling-het-grootste-gevaar-voor-privacy-opinie.

12 In de digitale omgeving betreffen het in wezen de bekende 'nullen en enen' die de 'machinetaal' zijn en een voor de computer/processor uitvoerbare code vormen om het woord of cijfer weer te geven in voor de mens vatbare en bruikbare vorm.

13 Volgens Van Dale wordt onder data verstaan: gegevens, zoals vastgelegde feiten. Onder informatie: het vragen respectievelijk verschaffen van kennis en inzicht.

14 Hof Den Haag 19 februari 1981, *TvGR* 1981/11.

15 Hof Den Bosch 6 juli 1987, *TvGR* 1988/19.

In een geschil tussen een cosmetisch chirurg en een privékliniek oordeelde de Hoge Raad in 2012 dat zowel de instelling als de zelfstandig (niet in loondienst werkzame) hulpverlener (chirurg) beide worden aangemerkt als hulpverlener in de zin van de Wet op de geneeskundige behandelingsovereenkomst (WGBO). Op iedere hulpverlener rust de dossierplicht van artikel 7:454 BW. Om die reden had de chirurg volgens de Hoge Raad recht op afgifte van kopieën van de door hem behandelde patiënten.[16] Het eigendomsrecht van medische dossiers, in welke vorm (fysiek of digitaal) dan ook, ligt derhalve primair bij de hulpverlener. Bovenberg gebruikt in zijn dissertatie, *Property rights in blood, genes and data. Naturally yours*, bij de beantwoording van de vraag wie eigenaar is van DNA en onderzoek dat is gedaan met DNA, de Databankenwet en Databankenrichtlijn (waarover hieronder nader meer) om eigenaarschap te bepalen.[17]

Aan wie behoren data dan toe? In feite komt het erop neer dat degene (natuurlijk persoon of rechtspersoon) die de servers beheert en/of eigenaar is van de harde schijven waarop de data staan of van de sensoren die de data verwerken én daar (technische of juridische) controle over en toegang toe heeft, kan bepalen wie wat met die data mag doen en zich daarmee *de facto* als eigenaar kan gedragen. Indien diegene een substantiële investering in kwantitatief of kwalitatief opzicht in de verkrijging of samenstelling van de data kan aantonen, wordt hij juridisch additioneel beschermd door het databankenrecht. Anderzijds, indien de data persoonsgegevens bevatten, kan hij gedwongen worden de data aan te passen of te vernietigen. Zulks op grond van de privacywet- en -regelgeving.[18] In die zin is het eigenaarschap niet absoluut.

Medische (persoons)gegevens

In de zorg wordt de term medische gegevens veelvuldig gebruikt. De vraag is wat wordt daaronder verstaan. Er bestaat geen algemeen aanvaarde definitie van de term medisch gegeven. Volgens de aanstaande Europese Algemene Verorde-

16 HR 25 mei 2012, LJN BV8508.

17 J.A. Bovenberg, *Property rights in blood, genes and data. Naturally yours* (diss. UL), Leiden/Boston, Martinus Nijhof Publishers, 2006.

18 Art. 36 Wbp: 'Degene aan wie overeenkomstig artikel 35 kennis is gegeven van hem betreffende persoonsgegevens, kan de verantwoordelijke verzoeken deze te verbeteren, aan te vullen, te verwijderen, of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen'. In de zaak Google Spain and Google Inc v Agencia Espanola de Proteccion de Datos *of* Mario Costeja Gonzalez, mei 2014, bepaalde het Europese Hof van Justitie, 'the individual has the right to request the removal from an internet search engine of information which relates to that individual, and that the individual's right to data protection 'will override the economic interest' (i.e. the property right) 'of the operator of the search engine'.

ning Gegevensbescherming (AVG)[19], waarover in paragraaf 5 meer, zijn persoonsgegevens: 'gegevens die betrekking hebben op een (..) persoon die direct of indirect, met behulp van middelen waarvan mag worden aangenomen dat zij redelijkerwijs de door de voor de verwerking verantwoordelijke dan wel door een andere natuurlijke of rechtspersoon in te zetten zijn, kan worden geïdentificeerd, met name aan de hand van een identificatienummer, gegevens over de verblijfplaats, een online-identificatiemiddel of een of meer specifieke elementen die kenmerkend zijn voor zijn fysieke, fysiologische, genetische, mentale, economische, culturele of sociale identiteit.' (art. 4, lid 3, sub 1 AVG).

Medische gegevens, indien en voor zover eenvoudig herleidbaar tot een natuurlijk persoon, zijn (gezien deze definitie) persoonsgegevens en vallen derhalve direct onder de werking van de AVG. Dit in tegenstelling tot de Wbp waarbij het begrip persoonsgegevens een algemene definitie kent en in artikel 16 bepaalde persoonsgegevens, zogenoemde gevoelige persoonsgegevens, waaronder gegevens over iemands gezondheid, onder een strenger regime worden geplaatst, namelijk waarvoor in beginsel een verwerkingsverbod geldt.

4 Bronnen en opslagplaatsen van data

Bij big data in de zorg draait het niet enkel om 'medische persoonsgegevens', maar om allerlei soorten gegevens uit uiteenlopende bronnen, zoals data uit het publieke en het sociale domein en omgevingsdata. Het gaat globaal om vijf categorieën data:

- *human generated data* (door zorgverleners in huisartsinformatiesystemen (HIS) en ziekenhuisinformatiesystemen (ZIS) in elektronische patiëntendossiers (EPD) vastgelegde aantekeningen en e-mails);
- transactiegegevens (zoals declaraties en DBC's);
- biometrische gegevens (zoals CT- en MRI-scans, röntgenfoto's, fysiologische meetgegevens);
- *machine-to-machine data* (door sensoren en bewakingsapparatuur gegenereerde gegevens);
- websites en sociale media.[20]

In talloze wearables, zoals 'Fitbit', apps en op servers en platformen die door zorgaanbieders, de overheid maar ook de industrie aan het publiek wordt aangeboden, zoals eHealthzelfzorg-apps, staan inmiddels ook miljarden gegevens die betrekking hebben op iemands gezondheid. Veelal is niet bekend waar welke data

19 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf.

20 *Transforming Health Care Through Big Data, Strategies for leveraging big data in health care industry*, Institute for Health Technology Transformation, 2013, p. 6.

staan opgeslagen of indien er sprake is van 'data in motion'. Men spreekt daarbij dan wel over cloud computing.[21]

Medisch-wetenschappelijk onderzoek richt zich in toenemende mate op de betekenis van genetische en omgevingsfactoren bij veelvoorkomende (multifactoriële) aandoeningen. Hiervoor zijn grootschalige collecties van data en lichaamsmaterialen nodig. Deze worden opgeslagen in biobanken. Biobanken zijn in het algemeen grootschalig, hebben brede onderzoeksdoelstellingen en stellen daarvoor gegevens en materiaal aan onderzoekers in binnen- en buitenland beschikbaar. Het gaat daarbij veelal om langdurige bewaring van niet geanonimiseerde[22] materialen en (genetische) gegevens.[23]
Is big data en/of de omgang met deze data gereguleerd en zo ja hoe? Hier ga ik in de navolgende paragraaf nader op in.

5 Juridisch kader

In deze paragraaf zal het huidige en aanstaande juridisch kader dat betrekking heeft of kan hebben op big data en het recht op privacy en gegevensbescherming worden besproken. Op dit moment is er nog geen specifieke Europese of Nederlandse wetgeving die big data en het gebruik van bigdatatechnieken reguleert. Wel zijn er algemene (huidige en toekomstige) privacy- en gezondheidszorgwetten en -regels en intellectuele-eigendomswetten die samen een kader scheppen. Op big data is geen of steeds andere (toezichts)wet- en -regelgeving van toepassing. Dit roept de vraag op wie verantwoordelijk of aansprakelijk is voor de gegevens en de verdere verwerking ervan in het geval van bigdatatoepassingen. Dit terwijl deze verwerkingen gevoelige persoonsgegevens, zoals medische gegevens, (kunnen) betreffen. In haar rapport 'Big Data in een vrije samenleving' stelt de WRR dat de huidige regels de burger onvoldoende beschermen.[24]

Bij big data gaat om het hergebruiken (secundaire toepassing) van data voor de hierboven genoemde 'kansen'. Veelal zullen daar data bij betrokken zijn die, een-

21 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

22 Er wordt wel veelvuldig gebruikgemaakt van pseudonimisatie, waarbij de identiteit van een natuurlijk persoon op wie de materialen betrekking heeft, is versleuteld.

23 M.C. Ploem, 'Gegeven voor de wetenschap; Regulering van onderzoek met gegevens, lichaamsmateriaal en biobanken', in: *Wetenschappelijk onderzoek in de zorg*. Preadvies Vereniging voor Gezondheidsrecht, 2010, Den Haag, Sdu Uitgevers 2010, p. 169.

24 *Big Data in een vrije en veilige samenleving*, Wetenschappelijke Raad voor het Regeringsbeleid, Amsterdam University Press, 2016.

voudig, tot een individu herleidbaar zijn of zal het toepassen van big data impact hebben op de persoonlijke levenssfeer van de burger, of – in het zorgproces –, de patiënt.
Voordat zal worden ingegaan op de huidige en aanstaande formele wet- en regelgeving zal ik eerst nader ingaan op het privacy begrip.

5.1 Het privacybegrip mondiaal

Er zijn in de wereld meerdere 'modellen' waar het gaat om privacywetgeving. Dit is in dit verband relevant omdat de data niet alleen in Europa, maar wereldwijd verwerkt zal (kunnen) gaan worden waar het gaat om bigdatatoepassingen.

Verenigde Staten van Amerika
In de VS geldt als uitgangspunt dat zodra een individu gegevens die op hem of haar betrekking hebben aan een organisatie verschaft, die organisatie zich eigenaar van die data mag noemen. Tenzij er sectorspecifieke wet- en regelgeving zich tegen een bepaalde verwerking verzet, bijvoorbeeld HIPAA (The Health Insurance Portability and Accountability Act of 1996)[25], staat het de organisatie vrij te bepalen wat het met de persoonsgegevens doet.

Apec
In de *Asian-Pacific*-regio is het leidende concept dat van 'accountability'.[26] Dit betreft een, naar onze termen, samenstel van verantwoordelijkheid en aansprakelijkheid. Organisaties zijn verplicht maatregelen te incorporeren die bescherming bieden tegen schade aan individuen en het oneigenlijk verzamelen en gebruik van persoonsgegevens.

Europa
In de EU geldt het zelfbeschikkingsrecht van het individu als een voornaam uitgangspunt. Dit is vastgelegd in onder meer het EU Handvest, het EVRM en de Grondwet. De organisatie ('data controller' oftewel 'verantwoordelijke') is verplicht doeltreffende maatregelen te treffen ter bescherming van persoonsgegevens, welke maatregelen tevens moeten inhouden dat de persoonsgegevens alleen worden gebruikt op een wijze zoals toegestaan door het individu (de 'betrokkene') of zoals is bepaald bij wet.

5.2 De ontstaansgeschiedenis van de belangrijkste privacyprincipes

Het definiëren van het recht op privacy is niet rechttoe-rechtaan en kent een lange geschiedenis. Sinds 1890 is het begrip door culturele, juridische en filosofi-

25 http://www.hhs.gov/hipaa/.
26 http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

sche invloeden vormgegeven. Voor zover bekend is *'the Right to Privacy'* voor het eerst in 1890 door Warren en Brandeis geïntroduceerd in een artikel in *Harvard Law Review*. In feite kwam hun betoog erop neer dat privacy inhoudt: *the right to be left alone*.[27] In 1950 werden in *EU Convention of Human Rights* reeds snelle technologische ontwikkelingen genoemd die de privacy zouden kunnen schaden en werd de stap naar informationele privacy gezet. In 1980 publiceerde de OECD Data Protection Guidelines[28]. Het doel van de richtlijnen was: '*to help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it*'. De uit de richtlijnen voortvloeiende minimumstandaarden, te weten: 1. Collection Limitation Principle, 2. Data Quality Principle, 3. Purpose Specification Principle, 4. Use Limitation Principle, 5. Security Safeguards Principle, 6. Openness Principle, 7. Individual Participation Principle en 8. Accountability Principle, zijn wereldwijd breed overgenomen in nationale en multinationale wet- en regelgeving. In 1984 beschreef filosoof F. Schoeman '*the ability of an individual to control the access that others have to personal information*'. Het recht op collectieve privacy werd voor het eerst opgevoerd in 1967 door dr. Alan F. Westin, '*privacy is the claim of individuals, groups, or institutions to determine when, how and to what extent information about them is communicated to others*'.[29] De Europese Privacyrichtlijn[30] stamt uit 1995, de tijd waarin het internet langzaamaan op gang kwam. De Privacyrichtlijn is goeddeels gebaseerd op de OECD-richtlijnen.

5.3 Het huidige kader in Europa en Nederland

Het begrip persoonsgegevens wordt in de Europese Privacyrichtlijn omschreven als 'alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'. Of een persoon kan worden geïdentificeerd zal afhangen van de mogelijkheden van de techniek in het concrete geval. Met de voortschrijdende informatietechnologie, waaronder bigdatatechnieken, nemen deze mogelijkheden – en daarmee de kans op identificatie – sterk toe. Het onderscheid tussen persoonsgegevens en gegevens niet zijnde persoonsgegevens is strikt genomen nu nog relevant omdat dit van invloed is op de toepasselijkheid van deze wet- en regel-

27 *Harvard Law Review* 4 (5), 193-220, 1890.

28 http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

29 *Privacy and Freedom*, New York 1967.

30 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:nl:HTML).

geving. Echter, zoals uit paragraaf 6 van de bijdrage van Ottes bleek, wordt het steeds eenvoudiger gegevens te de-anonimiseren door het koppelen van gegevens uit meerdere bronnen.
De belangrijkste wetten en regelingen met betrekking tot de verwerking van medische persoonsgegevens en het beroepsgeheim zijn vervat in, om en nabij, achttien formele wetten, veldnormen (zoals NEN 7510 e.v.), (Europese) richtlijnen en handreikingen die regels of kaders stellen. De belangrijkste formele wet- en regelgeving wordt hier genoemd. Het gebruik van medische persoonsgegevens in het kader van de behandeling van de patiënt wordt primair beheerst door de WGBO (opgenomen in titel 7, afdeling 5 van Boek 7 BW, art. 446-468), Wet op de beroepen in de individuele gezondheidszorg (Wet BIG), Wet kwaliteit, klachten en geschillen zorg (Wkkgz), Wet gebruik burgerservicenummer in de zorg (Wet BSN-z) en de Wet bescherming persoonsgegevens (Wbp). In het navolgende zal ik kort de relevantie van voornoemde regelingen bespreken.

WGBO
Zoals de lezer bekend zal zijn behelst artikel 7:454 BW de dossierplicht van de hulpverlener. Er zijn geen vormvereisten voor het dossier: zowel elektronische als fysieke opslag is mogelijk. Op grond van artikel 7:455 BW rust de plicht op zorgaanbieders het patiëntendossier minimaal vijftien jaar te bewaren. De patiënt heeft het recht om vóór afloop van deze termijn vernietiging van (delen van) het op hem betrekking hebbende dossier te vorderen, tenzij de wet of de eisen van goed hulpverlenerschap zich hiertegen verzetten of redelijkerwijs aannemelijk is dat verdere bewaring van aanmerkelijk belang is voor een ander dan de patiënt. Bij de totstandkoming van de WGBO heeft de wetgever big data of voor het publieke belang relevante toepassingen niet overwogen als 'een aanmerkelijk belang voor een ander dan de patiënt'. Artikel 7:457 BW regelt het medisch beroepsgeheim. Zorgaanbieders moeten erop toezien dat anderen geen toegang krijgen tot de gegevens die zijn opgeslagen in het dossier, tenzij de patiënt hier toestemming voor verleent. In afwijking van het toestemmingsvereiste uit artikel 7:457 BW, regelt artikel 7:458 BW het gebruik van medische persoonsgegevens, zónder toestemming van de patiënt, die zijn vergaard in het kader van een geneeskundige behandelingsovereenkomst voor wetenschappelijk onderzoek. Dit recht komt evenwel uitsluitend de hulpverlener toe. In de WGBO is een bepaling opgenomen over onderzoek met anoniem lichaamsmateriaal (art. 7:467 BW). De bepaling houdt in dat onderzoek met niet-herleidbaar lichaamsmateriaal, dat tijdens de behandeling is vrijgekomen, is toegestaan mits de patiënt geen bezwaar heeft gemaakt en het onderzoek met de vereiste zorgvuldigheid wordt verricht. Uit de MvT volgt dat bij wetenschappelijk onderzoek met herleidbaar lichaamsmateriaal van een verdergaand toestemmingssysteem moet worden uitgegaan.[31]

31 E.J. Kranendonk, 'Kind en biobank: enkele juridische aspecten', *TvGR* 2013. (37) 3, p. 273-274.

Wet BIG
Artikel 88 Wet BIG omvat de geheimhoudingsplicht van BIG-geregistreerde zorghulpverleners. Het niet-naleven van de verplichting kan onder andere leiden tot een tuchtmaatregel, vervolging en/of een bestuurlijke boete. Kort en goed: een hulpverlener kan niet zonder meer patiëntgegevens ter beschikking stellen voor bigdatatoepassingen, zonder dat hij of zij zich ervan heeft vergewist dat hij zijn of haar beroepsgeheim niet doorbreekt, althans de patiënt daarvoor toestemming heeft gegeven.

Wkkgz
De Wkkgz heeft per 1 januari 2016 onder meer de Kwaliteitswet zorginstellingen vervangen. Waar deze laatste wet het verlenen van 'verantwoorde zorg' als uitgangspunt kende, betreft dat in de Wkkgz 'goede zorg'. Artikel 2 Wkkgz bepaalt dat onder goede zorg wordt verstaan: 'zorg van goede kwaliteit en van goed niveau die in ieder geval veilig, doeltreffend, doelmatig en cliëntgericht is, tijdig wordt verleend, en is afgestemd op de reële behoefte van de cliënt'. Artikel 3 Wkkgz betreft een nadere invulling van artikel 2. De Inspectie voor de Gezondheidszorg (IGZ) bepaalde in 2008 dat de normen zoals vastgelegd in NEN 7510 en artikel 13 Wbp – het tenuitvoerleggen van passende technische en organisatorische maatregelen door de verantwoordelijke – invulling geven aan het begrip 'verantwoorde zorg' conform artikel 2 Kwaliteitswet zorginstellingen. Ik ga ervan uit dat deze normen ook invulling geven aan het begrip 'goede zorg' conform artikel 2 Wkkgz, aangezien 'verantwoorde zorg' en 'goede zorg' op essentiële punten overeenstemmen. Het toepassen van big data door een zorginstelling dient te passen binnen de open norm van goede zorg. Dit is in de Wkkgz niet verder uitgewerkt.

Wet BSN-z
Conform de artikelen 4 tot en met 9 Wet BSN-z is een zorgaanbieder verplicht zijn medische dossiers te koppelen aan een burgerservicenummer. Door deze koppeling is er vrijwel altijd sprake van tot een individu herleidbare informatie en derhalve van persoonsgegevens.

Wbp
De Wbp betreft de Nederlandse implementatie van de Privacyrichtlijn. Artikel 1 sub a Wbp bepaalt dat de Wbp slechts van toepassing is op persoonsgegevens. Dat impliceert gegevensverwerking op individueel niveau. Dit in vergelijking met big data waar gegevensverwerking veelal op collectief niveau plaatsvindt. Het gebruik van groepsprofielen, bijvoorbeeld de constatering dat alle jongeren onder de 21 een grotere kans op alcoholvergiftiging hebben, valt niet rechtstreeks onder de Wbp. Waar voor het opstellen van deze profielen vaak wel persoonsgegevens nodig zijn, is de toepassing – mits niet toegepast op een individu – niet gereguleerd door de Wbp. De Wbp wordt medio 2018 vervangen door de AVG.[32]

32 Art. 46 Uitvoeringswet Algemene verordening gegevensbescherming.

Overige wet en regelgeving
De hiervoor genoemde wet- en regelgeving zag met name op de individuele gezondheidszorg, waar binnen de kring van behandelaars en hulppersonen reeds op grote schaal uitwisseling van medische gegevens, waaronder persoonsgegevens plaatsvindt. Buiten de kring van behandelaars en hulppersonen (collectieve/publieke gezondheidszorg) vinden er nog meer uitwisselingen plaats, zoals in de sociale-, ggz- en publieke gezondheidsdomeinen. Deze uitwisselingen worden primair beheerst door de Wet maatschappelijke ondersteuning (Wmo), Jeugdwet (Jw), Wet marktordening gezondheidszorg (Wmg), Wet medisch-wetenschappelijk onderzoek bij mensen (WMO), Wet bijzondere opneming in psychiatrische ziekenhuizen (Wet Bopz) en de zorgverzekeringswet (Zvw). Deze wetten geven alle geen specifieke regels over big data.

Tevens kan op data of informatie intellectuele-eigendomswetgeving (IE-wetgeving) van toepassing zijn, zoals de Databankenwet (Dw) of de Auteurswet (Aw). De Dw en Aw verschaffen de 'producent' van een databank respectievelijk 'maker' van een auteursrechtelijk beschermd 'werk' een exclusief recht tot openbaarmaking en verveelvoudiging c.q. exploitatie daarvan. De Databankenwet is van toepassing indien sprake is van een verzameling van gegevens, waarvan de verkrijging, controle of presentatie in kwalitatief of kwantitatief opzicht getuigt van een substantiële investering.[33] Voor auteursrechtelijke bescherming geldt dat er sprake moet zijn van een 'werk' met een 'eigen, oorspronkelijk karakter dat het persoonlijk stempel van de maker draagt'.[34] De drempel voor auteursrechtelijke bescherming van een 'werk' (dit kan een stuk tekst zijn, maar ook een computerprogramma) ligt laag.[35] Dat wil zeggen dat auteursrecht relatief snel wordt aangenomen.

Aanstaande wet- en regelgeving
Er staat ook de nodige nieuwe relevante (formele) wet- en regelgeving op stapel. De Europese en Nederlandse wetgever hebben zich tot doel gesteld de privacy en rechtspositie van de burger (in het zorgproces: de patiënt) in de informatiemaatschappij te versterken én tegelijkertijd de digitale economie te bevorderen. De meest in het oog springende nieuwe wet- en regelgeving in dit verband is de AVG. Deze verordening zal rechtstreekse werking hebben en omvat meer dan 80 nieuwe vereisten ten opzicht van de Privacyrichtlijn en de Wbp. De meest relevante vereisten voor verwerking van persoonsgegevens in de bigdatacontext betreffen:

---

33 Art. 1 lid 1 sub a Dw.
34 HR 4 januari 1991, *NJ* 1991/608, Van Dale/Romme.
35 ECJ 16 juli 2009 http://curia.europa.eu/juris/document/document.jsf?docid=72482&doclang=NL (*Infopaq)* en Hoge Raad 30 mei 2008 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2008:BC215 (*Endstra*).

1. het recht om niet te worden onderworpen aan een louter op geautomatiseerde verwerking gebaseerd besluit;
2. het recht op inzage;
3. het recht om vergeten te worden;
4. het principe van *Data protection by Design*;
5. de verplichting om een *Privacy Impact Assessment* (PIA) uit te voeren voorafgaand aan de verwerking van persoonsgegevens (zoals een bigdatatoepassing); en
6. de verplichting om betrokkenen te informeren over de bewaartermijn van de persoonsgegevens.

Ad 1.
Artikel 22 AVG bepaalt dat de betrokkene het recht heeft niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder *profiling*, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft. Tegelijkertijd worden uitzonderingen gegeven op basis waarvan *profiling* is toegestaan, namelijk wanneer het opstellen van een profiel nodig is voor de uitoefening van een overeenkomst, als het is toegestaan op grond van de wet of in het geval het individu toestemming heeft gegeven voor *profiling*.

Ad 2. en ad 6.
Het recht op inzage, artikel 15 AVG, is gedetailleerder dan het inzagerecht dat nu geldt onder de Wbp. Onder andere het recht op inzage in de logica van geautomatiseerde besluitvorming op basis van persoonsgegevens is uitgebreid. Zoals gezegd worden beslissingsregels in het kader van big data gegenereerd door algoritmes die niet altijd worden begrepen door de partijen die er gebruik van maken (zie nader onder 6.2). Naast inzage in de beslissingsregels moet de verantwoordelijke ook inzicht geven in de impact en de consequenties van de geautomatiseerde besluitvorming. Conform overweging 63 valt het meedelen van bewaartermijn onder het inzagerecht. Indien mogelijk moet de bewaartermijn worden gemeld aan de betrokkene. Ook dit blijkt lastig bij de inzet van bigdatatechnieken. Omdat bestanden veelal aan elkaar zijn gekoppeld waarbij verschillende verantwoordelijken in het spel zijn, zijn bewaartermijnen moeilijk te achterhalen. Niet alleen is het welhaast ondoenlijk voor de betrokkenen alle verantwoordelijken te achterhalen, zij kunnen ook allemaal andere bewaartermijnen hanteren.

Ad 3.
Het 'recht om vergeten te worden' is vastgelegd in artikel 17 AVG. Dit is echter geen absoluut recht. Volgens de Hoge Raad kunnen er goede redenen zijn gegevens te blijven bewaren. In de context van big data heeft dit recht grote gevolgen. Om persoonsgegevens op verzoek te verwijderen moet men ook weten waar die persoonsgegevens zich precies bevinden. In het bigdatalandschap zal dit veel

moeite kosten. Niet alleen gaat het om grote hoeveelheden data, maar deze worden gekoppeld, door verschillende partijen verwerkt, en dat meestal op snelheid.

Ad 4.
Artikel 25 AVG regelt *Privacy by Design* – gegevensbescherming door ontwerp. Afhankelijk van onder andere de waarschijnlijkheid en ernst van uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, moeten zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, technische en organisatorische maatregelen worden getroffen door de verwerkingsverantwoordelijke.

Ad 5.
Er wordt een verplichte 'gegevensbeschermingseffectbeoordeling' ingevoerd (*Data protection impact assessment*, ex artikel 35 AVG). Deze beoordeling dient vooraf aan een verwerking van persoonsgegevens plaats te vinden om effecten (risico's) van de beoogde verwerkingsactiviteit in kaart te brengen. Naar aanleiding hiervan kunnen en/of moeten maatregelen worden getroffen om eventuele privacyrisico's op te vangen. Artikel 35 lid 3 sub a AVG verplicht een gegevensbeschermingseffectbeoordeling indien bigdatatechnieken worden gebruikt voor het verwerken van persoonsgegevens.

Niet-naleving van de verplichtingen op grond van de AVG kan gesanctioneerd worden met boetes die kunnen oplopen tot € 20.000.000 of 4 procent van de omzet van de 'verantwoordelijke'.

Ook op nationaal niveau is nieuwe wetgeving in de maak. De Eerste Kamer heeft 4 oktober 2016 ingestemd met de Wet cliëntenrechten bij elektronische verwerking van gegevens (Wet cliëntenrechten).[36] Op grond van artikel 15a lid 2 Wet cliëntenrechten moet de cliënt de keuze worden gegeven toestemming te geven dat alle of bepaalde persoonsgegevens van hem of haar via een elektronisch uitwisselingssysteem beschikbaar worden gesteld aan bepaalde zorgaanbieders of categorieën van zorgaanbieders. Door afscheid te nemen van de generieke *opt-in* wordt hiermee beoogd dat voor de cliënt duidelijker wordt wie tot welke medische persoonsgegevens toegang heeft. Artikel 15d Wet cliëntenrechten regelt het recht tot inzage of afschrift van het dossier van de cliënt, of van de gegevens betreffende deze cliënt die de zorgaanbieder via een elektronisch uitwisselingssysteem beschikbaar stelt. Minister Schippers erkent dat dit wetsartikel gevoelig ligt in het licht van big data. Zij gaf nadrukkelijk aan dat het wetsvoorstel niet regelt wat de patiënt doet met de door hem opgevraagde gegevens: 'Dit kan problematisch zijn

36 Volgens art. 25 dient de wet aangehaald te worden als: Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.

als de gegevens bij derden komen, bijvoorbeeld bigdatabedrijven die niet onder het beroepsgeheim vallen'.[37]

6 Knelpunten

In het navolgende wordt ingegaan op enkele praktische en juridische knelpunten waar het gaat om big data in de zorg binnen het huidige juridische raamwerk.

6.1 De Wbp en WGBO beschermen het individu niet effectief bij big data

Zoals uit deel IA is gebleken, maakt big data een intensievere observatie van ons leven mogelijk, terwijl een aanzienlijk deel van de wet- en regelgeving (voornoemd) om de privacy te beschermen er vrijwel betekenisloos door is geworden. Big data holt ook de belangrijke techniek van het anonimiseren van gegevens uit. Daar komt bij dat bigdatavoorspellingen invloed kunnen hebben op toekomstig gedrag van het individu. Ook bestaat het reële risico dat bigdata-actoren in het zorgproces bigdatatechnieken inzetten op plaatsen die daarvoor niet echt geschikt zijn of te veel te vertrouwen in de resultaten van bigdata-analyses.
Hoe verhoudt dit zich tot de huidige wet- en regelgeving, zoals de Wbp? Bij big data is degene die het doel en de middelen bepaalt (de 'verantwoordelijke' in de zin van de Wbp) veelal een dynamisch groep van diverse (rechts)personen. Het kan voorkomen dat meerdere partijen meerdere doelen bepalen. Hergebruik wringt met het basisprincipe dataminimalisatie uit artikel 7 Wbp: 'Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld'. Ook wringt het met een ander basisprincipe uit de Wbp: doelbinding. Dit is neergelegd in artikel 9 lid 1 Wbp: 'Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen'. Artikel 11 Wbp bepaalt dat de verantwoordelijke de nodige maatregelen moet treffen om te waarborgen dat persoonsgegevens juist en nauwkeurig zijn. Dit houdt in dat de verantwoordelijke alleen profielen mag creëren of toepassen op een individu die juist en nauwkeurig zijn. Dit is door het dynamische karakter van big data vaak onmogelijk. Het nemen van technische en organisatorische maatregelen conform artikel 13 Wbp blijkt lastig uitvoerbaar en niet te controleren te zijn in de praktijk. (Veel) verschillende entiteiten verwerken medische gegevens en voegen deze samen uit verschillende bronnen zonder dat hier een juridische grondslag voor is en het transparantiebeginsel wordt nageleefd. Betrokkenen weten veelal niet dat hun medische gegevens worden verzameld en/of hun rechten zijn aangetast en kunnen om die reden geen beroep doen op het recht op informatie. Persoonlijke schade of belang aantonen blijkt lastig. Dit

37 https://www.eerstekamer.nl/nieuws/20160929/debat_over_patientenrechten.

druist in tegen het transparantiebeginsel ex artikelen 33 en 34 Wbp. Bijzondere – sectorale – wetten waar wordt afgeweken van de Wbp, bijvoorbeeld in de WGBO, bevatten doorgaans een op de sector toegespitste nadere precisering van de algemene regel en gelden uit dien hoofde als een *lex specialis* ten opzichte van de Wbp. De specialis wijkt niet af van de algemene regel maar bedoelt daaraan een nadere invulling te geven voor de desbetreffende – in dit geval medische – sector. Voor zover in de andere wettelijke voorschriften over een of meerdere aspecten van de verwerking van persoonsgegevens geen meer concrete regeling is getroffen, is de Wbp weer aanvullend van toepassing.[38] Echter ook in de WGBO is geen specifieke op zorgbigdata toe te passen regeling opgenomen.

6.2 Spanningsveld tussen grondrechten van het individu en de macht die private partijen verkrijgen over zorgdata

Bezit van data

Zoals aangegeven worden op grote schaal medische gegevens verzameld en opgeslagen. Ook door private partijen zoals Google, Microsoft, IBM en Apple. Maar ook een bedrijf als Philips richt zich meer op de data dan op de hardware.[39] Het risico hierbij is dat bepaalde zorginformatie en data, zodra in private handen, niet meer vrijelijk beschikbaar zijn c.q. niet meer beschikbaar zijn ten behoeve van het individu of het publieke belang, zoals wetenschappelijk onderzoek. Het is daarbij niet ondenkbaar dat er, net als bij zoekmachines op internet, één of enkele dominante partijen komen, waardoor centralisatie van kennis ontstaat – een alomvattende *corpus of knowledge* – die in private handen is. Immers, de private bedrijven beheersen de servers/platformen waarop de data staat, bepalen wie en onder welke voorwaarden daar toegang tot krijgt en welke vorm van (her)gebruik is toegestaan. Dit gebeurt op basis van eenzijdige algemene gebruiksvoorwaarden. Ook is er een ontwikkeling gaande waarbij de richting van kennisexploitatie meer en meer privaat wordt gestuurd. Zo wordt al veel klinisch onderzoek, met name *randomized controlled trials*, gefinancierd door de farmaceutische industrie. Tevens kunnen deze bedrijven zich wellicht beroepen op exclusieve IE-rechten, zoals het databanken- en auteursrecht. Als al deze gegevensstromen via private partijen lopen zal er commerciële invloed zijn op de richting en wijze waarop kennis en

38 *Kamerstukken II* 1997-1998, 25892, nr.3, blz. 126.

39 Philips' HealthSuite device cloud links over 7 million healthcare devices and sensors in conjunction with social media and electronic medical health record data to a range of backend data stores and front-end applications for disease prevention and social healthcare provision. It collects all of the data for analysis and to help generate algorithms to improve the quality of the medical advice that can be generated from it; it also opens those data stores to developers, which can tap into the cloud service using purpose-built API's. In: http://www.businesscloudnews.com/2015/06/04/philips-health-cloud-lead-privacy-compliance-upgradability-shaping-iot-architecture/.

kennislacunes worden opgevuld.[40] Het individu heeft hier geen inzicht in, laat staan controle over. Noch in technische noch in juridische zin.

Controle over algoritmes
Beslissingen die op basis van big data worden gemaakt zijn voorgerekend door algoritmes. Een algoritme kan gedefinieerd worden als: een geheel van regels voor het oplossen van een bepaald probleem in een bepaal aantal stappen, of als: een eindige reeks instructies, die vanuit een gegeven begintoestand naar een beoogd doel leiden. Toegepast op computerprogramma's zijn algoritmen reeksen van instructies die de computer zeggen wat te doen en hoe een bepaald eindresultaat te bereiken.[41] Algoritmes zijn geen wetten, in de zin dat zij niet door een wetgevende overheid zijn uitgevaardigd. Anderzijds blijken algoritmes wel normerend te werken en sturen zij het gedrag van mensen, zoals de wet dat doet.[42] Kenmerkend voor algoritmes is dat zij kunnen bijleren. De gegevens die waargenomen worden, worden gebruikt om het systeem bij te sturen. Een voorbeeld hiervan is een 'spamfilter'. In het algoritme is bepaald wat een 'goede' regel is en wat de voorwaarden of omstandigheden zijn om de bestaande regel aan te passen. Op basis van gedrag van de gebruiker, waarover voortdurend gegevens worden verzameld, wordt bepaald of het nodig is de regel aan te passen en wordt de regel aangepast aan de situatie. Er kleeft hier een groot risico aan. De berekeningen op basis waarvan algoritmes selecteren en kiezen zijn al zo complex dat niemand meer met 100 procent zekerheid kan zeggen of de uitkomsten kloppen. Laat staan dat deze door de mens zijn te controleren. Er is daarbij ook een duidelijk onderscheid te maken tussen de transparante, coöperatieve voorzijde van het internet en de dichte, ondoorzichtige achterzijde ervan, die wordt beheerst door slechts enkele ondernemingen met hun eigen (commerciële) belangen.[43] Ook algoritmes worden, net zoals data, niet beheerst of gereguleerd door wet- en regelgeving. Intern en extern toezicht op juistheid, integriteit en operationele doelmatigheid van algoritmes (en van de zuiverheid en representativiteit van de datasets waarmee ze gevoed worden) houdt geen gelijke tred met de steeds grootschaligere inzet van algoritmes in keuzes in het zorgproces.[44]

---

40 L. Ottes, *Big data in de zorg*, Wetenschappelijke Raad voor het Regeringsbeleid, Den Haag, 2016, p. 19. http://www.wrr.nl/fileadmin/nl/publicaties/PDF-Working_Papers/WP_19_Big_data_in_de_zorg.pdf.

41 Zie: http://computer.howstuffworks.com/question717.htm.

42 L. Dobush, *Algorithm Regulation #4: Algorithm as a Practice*, https://governancexborders.com/2013/01/14/algorithm-regulation-4-algorithm-as-a-practice/.

43 Zie: F. Stalder, *Between Democracy and Spectacle. The Front and Back of the Social Web*, http://felix.openflows.com/node/223.

44 A. Mikkers en J. Goudsmit, 'Door algoritmes voorgerekende keuzes leiden tot foute beslissingen', *FD*, 30 november 2016, p. 9.

6.3 Informed consent en de verschillende verschijningsvormen in de Wbp, WGBO, AVG en Wet cliëntenrecht

Uit de huidige en aanstaande wet- en regelgeving (Wbp, WGBO, AVG en Wet cliëntenrecht) zou kunnen worden afgeleid dat *informed consent* van de patiënt door de wet- en regelgever als panacee wordt beschouwd. Dat is geenszins het geval. Hoe verhouden de verschillende vormen van toestemming zich tot de inzet van big data? Waar geeft de betrokkene eigenlijk toestemming voor in geval van big data?

'Toestemming' is een verwerkingsgrondslag en principe dat zowel in de Privacyrichtlijn – en derhalve de Wbp – als in de WGBO ligt verankerd. Het vloeit voort uit het basisprincipe van het privacyrecht dat het individu mag bepalen wie, wanneer en waarvoor op hem/haar betrekking hebbende gegevens mag gebruiken. Eveneens is toestemming opgenomen in de AVG en Wet cliëntenrecht. Echter, in deze wetten wordt steeds een andere invulling gegeven aan het begrip toestemming. De ratio's van de wetten zijn ook verschillend. Waar de Privacyrichtlijn, Wbp en AVG informationele privacy van het individu waarborgen, reguleert de WGBO bijvoorbeeld de relatie tussen de zorghulpverlener en de patiënt in het kader van de behandeling van de patiënt.

De Wbp verbiedt het verwerken van persoonsgegevens betreffende iemands gezondheid, tenzij een beroep kan worden gedaan op een van de zes wettelijke uitzonderingen. Een daarvan is toestemming: Deze bijzondere persoonsgegevens mogen toch worden verwerkt als (a) de betrokkene 'uitdrukkelijke toestemming' heeft gegeven.[45] Onder uitdrukkelijke toestemming wordt verstaan 'elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden verwerkt'.[46] De artikel 29-werkgroep[47] publiceerde in 2007 een opinie[48] over 'uitdrukkelijke toestemming'. Daarin werd een aantal handvatten geboden voor de invulling van het

45 Art. 23 Wbp.

46 Art. 2 sub h Privacyrichtlijn.

47 De Artikel 29-werkgroep is het onafhankelijke advies -en overlegorgaan van Europese privacytoezichthouders. De werkgroep speelt een belangrijke rol in de totstandkoming van Europees beleid voor de bescherming van persoonsgegevens. De Artikel 29-werkgroep bestaat uit de nationale privacytoezichthouders van de lidstaten van de Europese Unie (EU) en de European Data Protection Supervisor (EDPS). De EDPS houdt toezicht op de verwerking van persoonsgegevens bij de instellingen en organen van de EU. De naam van de werkgroep is ontleend aan artikel 29 van de Privacyrichtlijn.

48 Werkdocument inzake de verwerking van persoonsgegevens betreffende de gezondheid in elektronische medische dossiers (EMD), 15 februari 2007 (WP131).

begrip. Allereerst moet toestemming uit vrije wil worden gegeven. Tevens moet toestemming 'specifiek' zijn wat inhoudt dat het betrekking moet hebben op een welbepaalde concrete situatie. Een 'algemeen akkoord' van de betrokkene om zijn of haar data in het EPD te plaatsen is te generiek. Het kaderen van specifieke toestemming is in de praktijk lastig: waar ligt de grens tussen specifieke en generieke toestemming? Ook moet toestemming op informatie berusten. Dat betekent dat de betrokkene zijn toestemming geeft op basis van beoordeling en begrip van de feiten en implicaties van een wijze van handelen. Het vereiste van geïnformeerde toestemming sluit tevens aan bij het algemene civiele recht. Artikel 3:36 BW en de daarop gebaseerde jurisprudentie worden ook op deze vorm van toestemming van toepassing geacht.[49] Uit de toelichting van de Autoriteit Persoonsgegevens (AP) op artikel 23 Wbp blijkt dat uit 'uitdrukkelijke' voortvloeit dat de betrokkene expliciet zijn wil omtrent verwerking dient te hebben geuit. Een stilzwijgende of impliciete toestemming is dan ook onvoldoende: de betrokkene dient in woord, schrift of gedrag uitdrukking te hebben gegeven aan zijn wil toestemming te verlenen aan de hem betreffende gegevensverwerking. Artikel 23 lid 2 Wbp bepaalt dat het verbod om persoonsgegevens te verwerken ten behoeve van wetenschappelijk onderzoek of statistiek niet van toepassing is voor zover het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost. Hieruit kan een trapsgewijs systeem worden afgeleid. In beginsel geldt een verbod op het verwerken van persoonsgegevens betreffende iemands gezondheid, ook ten behoeve van wetenschappelijk onderzoek of statistiek. Als uitzondering hierop geldt dat uitwisseling mag plaatsvinden met geïnformeerde toestemming van de patiënt. Pas wanneer toestemming niet mogelijk is en een uitzondering noodzakelijk is, komen andere uitzonderingen aan bod. Wanneer het gaat om een algemeen belang dat gegevensverwerking steeds rechtvaardigt, moet die afweging bij wet worden vastgelegd, bijvoorbeeld in de WGBO. Als het gaat om individuele belangen, volstaat in bepaalde gevallen ook een algemene regel die ruimte laat voor een individuele afweging.

Geïnformeerde toestemming voor het verwerken van medische gegevens is tevens vereist op grond van de WGBO. Zoals besproken in het juridische kader (paragraaf 5) kent de WGBO, als lex specialis, twee artikelen aangaande geïnformeerde toestemming: geïnformeerde toestemming conform artikel 7:448 jo. 7:450 BW die van toepassing zijn op het verrichten van geneeskundige handelingen en geïnformeerde toestemming op grond van artikel 7:457 BW welke ziet op het uitwisselen van medische gegevens. In deze bijdrage wordt enkel het laatste artikel behandeld en vergeleken met het toestemmingsvereiste uit de Wbp en Wet cliëntenrecht. Artikel 7:457 behelst het medisch beroepsgeheim en luidt als volgt: 'Onverminderd het in artikel 448 lid 3, tweede volzin, bepaalde draagt de hulpverlener zorg, dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel

49 *Kamerstukken II* 1997-1998, 25892, nr. 3, p. 151.

inzage in of afschrift van de bescheiden, bedoeld in artikel 454, worden verstrekt dan met toestemming van de patiënt. Indien verstrekking plaatsvindt, geschiedt deze slechts voor zover daardoor de persoonlijke levenssfeer van een ander niet wordt geschaad. De verstrekking kan geschieden zonder inachtneming van de beperkingen, bedoeld in de voorgaande volzinnen, indien het bij of krachtens de wet bepaalde daartoe verplicht.' Het artikel beschermt belangen zoals de vrije toegankelijkheid van de gezondheidszorg en de bescherming van de persoonlijke levenssfeer van de patiënt. De MvT bij het toestemmingsvereiste van de WGBO en de betreffende KNMG-richtlijnen zijn summier over de inhoud van dit vereiste. De KNMG stelt dat de patiënt slechts toestemming kan geven 'als hij vooraf is ingelicht over het doel, de inhoud en de mogelijke consequenties van de gegevensverstrekking'.[50] Het vooraf verstrekken van informatie wordt daarmee gezien als de kern van de toestemming. Om begrip over het doel, de inhoud en mogelijke consequenties te bewerkstelligen, dient informatie aan te sluiten bij de patiënt en moet het kernachtig en laagdrempelig worden weergegeven. Dit is met name belangrijk voor kwetsbare groepen zoals kinderen en ouderen.

De AVG voegt geen nieuwe vereisten toe maar benadrukt dat de toestemming uitdrukkelijk, op een passende wijze, vrij, specifiek en geïnformeerd moet worden gegeven *teneinde* te waarborgen dat de betrokkene zich bewust is van het feit dat hij toestemming voor gegevensverwerking geeft. Die bewustheid is dus het wezenskenmerk van de toestemming. De criteria die voor 'teneinde' genoemd worden, zijn de middelen om dat doel te bereiken. Ook de Wet cliëntenrecht stelt geen nieuwe vormvereisten aan het begrip toestemming. In artikel 15a en 15b Wet cliëntenrecht is de eis van 'uitdrukkelijke toestemming' neergelegd. Wel wordt een nieuwe invulling van het toestemmingsvereiste in artikel 15a lid 1 Wet cliëntenrecht geïntroduceerd: gespecificeerde toestemming. Dit ziet toe op hetgeen waarvoor toestemming wordt gegeven. Patiënten krijgen daarmee de mogelijkheid tot regie over wat in het dossier staat en bij wie welke gegevens komen; zij kunnen alle of bepaalde gegevens en bepaalde categorieën van zorgaanbieders uitsluiten van het medisch dossier, althans 'in theorie'. Voor zover een cliënt toestemming heeft gegeven, hoeft een zorgaanbieder niet opnieuw toestemming te vragen zijn gegevens uit te wisselen voor zover hij heeft kunnen vaststellen dat deze cliënt (generieke) toestemming heeft gegeven, en de desbetreffende zorgaanbieder niet heeft uitgesloten. In wezen concretiseert dit artikel de eis uit de Wbp dat toestemming specifiek moet zijn.

Ondanks de status van lex specialis ten opzichte van de Wbp, is het toestemmingsvereiste uit de WGBO minder gespecificeerd. Aangezien de vereisten die de Wbp stelt het meest concreet zijn, is deze wet op dit moment de belangrijkste

50 https://www.knmg.nl/richtlijn-omgaan-met-medische-gegevens, september 2016.

bron voor de invulling van het 'informed consent'. Bovendien geldt een strengere maatstaf vanuit de Wbp welke leidend is voor het antwoord op de vraag of een betrokkene toestemming geeft voor het verstrekken van medische persoonsgegevens. Voor zover uitdrukkelijke toestemming van de betrokkene ontbreekt, staan de Wbp en het medisch beroepsgeheim ex artikel 7:457 BW aan het verstrekken van deze gegevens in de weg.[51] Een ander verschil tussen de Wbp en WGBO is de zeggenschap. Waar de Wbp enkel gericht is op de betrokkene, de patiënt, ziet de WGBO ook op de arts: de arts heeft het laatste woord met een afweging van alle betrokken belangen. Het uitgangspunt dat degene wiens persoonsgegevens het betreft ook de zeggenschap over die gegevens behoort te hebben, wint echter ook voor het beroepsgeheim aan belang. Dat blijkt onder andere uit de gespecificeerde toestemming op grond van de Wet cliëntenrecht. De bepalingen uit de Wet cliëntenrecht doen niets af aan de bestaande regels uit de WGBO en de Wbp. Uit de memorie van toelichting van de Wet cliëntenrecht volgt dat het wetsvoorstel een aanvulling vormt op de Wbp en WGBO en het maakt duidelijk welke extra rechten en waarborgen voor cliënten – patiënten – van toepassing zijn bij elektronische gegevensuitwisseling en de beschikbaarheid van gegevens via een elektronisch uitwisselingssysteem. Tevens legt de Wet cliëntenrecht de nadruk op het informeren van cliënten over de voor- en nadelen van het verlenen van toestemming om gegevens via een elektronisch uitwisselingssysteem beschikbaar te stellen, alsmede het eventueel toepassen van uitsluitingen.[52] Dit komt overeen met het uitgangspunt van toestemming onder de WGBO waar ook het meeste gewicht aan het informatieaspect wordt toegekend. 'Toestemming' door de patiënt is in het licht van het vorenstaande een juridisch en praktisch vrijwel niet uitvoerbare grondslag en beschermt daardoor de belangen van het individu niet daadwerkelijk.

7 De blik vooruit gericht

De hoeveelheid data neemt exponentieel toe. Net zoals de technologische mogelijkheden om meer te doen met die data. Anderzijds hebben we te maken met de grondrechten privacy, het recht op gegevensbescherming en het beroepsgeheim. Middels de AVG krijgen toezichthouders de bevoegdheid fikse boetes op te leggen aan organisaties die zich niet aan de AVG, inclusief 80 nieuwe verplichtingen, houden. De vraag is wat betekent dit voor het recht. Zoals Moerel zich al afvroeg in 2014, hoe dient de 'niet te reguleren toekomst' te worden gereguleerd?[53] Door de privacy- en gegevensbeschermingwet- en regelgeving? Laten we het aan de rechtspraak over? Of, door de marktwerking of de informatietechnologie zelf?

51 Rb. Rotterdam 29 september 2010, ECLI:NL:LBROT:2010:BN9944.
52 *Kamerstukken II* 2012/2013, 33 509, nr. 3, p. 13.
53 Moerel 2014, a.w. p. 25.

Vanuit juridisch en technisch optiek zijn er verschillende oplossingsrichtingen aangedragen de afgelopen jaren.

Moerel stelt voor om de AVG drastisch aan te passen door:
1. vergroten van de 'gerechtvaardigd belang grond' voor de verantwoordelijke om alle datacategorieën te mogen verwerken, alsmede in alle fases van de datalevenscyclus;
2. het toevoegen van een concrete eis voor transparantie bij keuzes voor de betrokkene en het verlenen van daadwerkelijke en effectieve toegang tot de data door de betrokkene;
3. het verantwoordelijk en aansprakelijk (kunnen) houden van de verantwoordelijke voor de gehele datalevenscyclus; en
4. het invoeren van technologie-impactassessments ('TIA's' in plaats van 'PIA's').

In hun preadvies voor de Nederlandse Juristen Vereniging, *Homo Digitalis*, (2016) gaan Moerel en Prins in op het feit dat in het bigdatatijdperk de doelbinding uit de vigerende privacywet- en -regelgeving niet werkbaar is. Hun inzet komt erop neer dat een toets aan de hand van een gerechtvaardigd belang bij de verzameling en (verdere) verwerking van gegevens een effectievere privacybescherming oplevert die meer legitimiteit geniet dan de beoordeling op basis van het huidige regime. Daarbij geven ze overigens expliciet aan dat zij geen voorstander zijn van het Amerikaanse *use based*-systeem, waarbij het verzamelen van gegevens vrij wordt gelaten en alleen het gebruik gereguleerd. De gedachte daarbij is dat de wetgever geen rol heeft bij het stellen van voorwaarden aan het verzamelen en combineren van data, maar pas normstellend optreedt in de gevallen dat gegevens worden gebruikt op een wijze die als misbruik wordt gekwalificeerd. Tegen deze benadering pleit dat hiermee de weg vrij is voor het onbeperkt verzamelen van gegevens, ook gevoelige gegevens, bijvoorbeeld door het plaatsen van *sniffers* op telecomnetwerken.

Nissenbaum[54] pleit voor een context-afhankelijke benadering van bescherming van het recht op privacy. Zij noemt dit een raamwerk van contextuele integriteit. Dit zou een doorbraak (moeten) betekenen voor de miljoenen onzichtbare en oncontroleerbare 'trade offs' tussen organisaties en betrokkenen, waarbij diensten worden betaald met persoonsgegevens c.q. privacy. Het uitgangspunt is hierbij de wilsovereenstemming over toelaatbare dataverwerkingen en niet tot geheimhouding en controle (zelfbeschikking) over de persoonsgegevens.

Mayer-Schönberger is van mening dat veranderingen aan bestaande regels niet voldoende zijn om de gevolgen van de opkomst van big data in de hand te houden en de risico's ervan te beperken. Volgens haar is voor het beschermen van

54 H. Niessenbaum, *Privacy in Context, Technology, Policy and the Integrity of Social Life*, Stanford Law Books, 2010, p. 186.

privacy nodig dat bigdatagebruikers meer verantwoordelijkheid nemen voor hun daden. Ook zal de samenleving het gehele rechtsstelsel moeten aanpassen om menselijke handelingsvrijheid te garanderen en mensen verantwoordelijk te kunnen stellen voor hun daden (van privacy naar aansprakelijkheid). Ten derde zullen er nieuwe instellingen en deskundigen (algoritmisten) nodig zijn om complexe algoritmes te interpreteren die aan bigdatabeslissingen ten grondslag liggen en mensen steunen die schade (zouden kunnen) lijden als gevolg van big data.[55]

Dit laatste sluit aan bij de roep van Mikkers en Goudsmit voor internationale afspraken over verantwoordings- en ontwikkelingseisen voor algoritmes. Zij doen een klemmend beroep op de overheid om de wet- en regelgeving met name op dit terrein te actualiseren.

Wat is wijsheid?
Het grootschalig wijzigen of het aanvullen van de formele wet- en regelgeving zal mijns inziens geen oplossing bieden voor de hiervoor geconstateerde knelpunten en onvolkomenheden. Daarvoor is het onderwerp en de ontstane situatie juridisch, organisatorisch en technisch te complex. Het probleem is dat wet- en regelgeving geen rekening houdt met de context en de diverse belangen van de (vaak vele) betrokken partijen, alsmede publieke en private belangen die geregeld tegenover elkaar staan, terwijl juist daar zich problemen (kunnen) voordoen. De markt lost deze problemen niet op en de belanghebbenden zijn niet allemaal voldoende (juridisch of economisch) bij machte hun gerechtvaardigde belang(en) adequaat te behartigen. Ik beschrijf hier drie oplossingsrichtingen, ter verdere discussie en uitwerking.

Op de eerste plaats is het van belang op basis van de huidige en toekomstige wet- en regelgeving additionele (lees: meer concrete en in de context geplaatste) kaders te stellen voor toepassing van big data in de zorg. Dit om de kansen (beter) te benutten, maar tegelijkertijd de risico's te mitigeren en waar zich problemen voordoen deze te managen. Deze kaders dienen bij voorkeur door het veld te worden vastgesteld onder regie van het Informatieberaad/Medmij.[56]

---

55 Schönberger en Cukier, a.w. p. 242 e.v.

56 Medmij is een samenwerkingsverband van brancheorganisaties, verenigingen van huisartsen, ziekenhuizen, apothekers, thuiszorgorganisaties, verpleeghuizen, zorgverzekeraars, patiënten en (lokale) overheden. Deze organisaties vormen samen het Informatieberaad Zorg. Patiëntenfederatie Nederland coördineert het MedMij-programma en vormt samen met Nictiz en het ministerie van VWS het uitvoerende programmateam. De stuurgroep – met daarin leden van het Informatieberaad Zorg – stuurt het programmateam aan. MedMij stelt spelregels op voor de manier waarop persoonlijke gezondheidsomgevingen gegevens uitwisselen met (zorg)organisaties. http://www.medmij.nl/organisatie/.

Op de tweede plaats zouden de overheid en degenen die beïnvloed worden door bigdatabeslissingen meer grip moeten krijgen op algoritmes. Dit is mijns inziens belangrijker en beter werkbaar dan proberen eigenaarschap en/of omgang met data via wetgeving te reguleren. Een aanpassing van de Auteurswet kan hier soelaas bieden. Algoritmes betreffen computerprogrammatuur. De Auteurswet is ex artikel 10 sub 12 van toepassing op computerprogramma's en voorbereidende materialen. Meer in het bijzonder geeft artikel 45l Aw degene die bevoegd is tot het verrichten van de in artikel 45i bedoelde handelingen (gebruik van de programmatuur), de bevoegdheid de werking van dat werk waar te nemen, te bestuderen en te testen teneinde de daaraan ten grondslag liggende ideeën en beginselen te achterhalen. Indien en voor zover algoritmes worden gebruikt voor beslissingen die invloed hebben op een individu of een groep van individuen, zou dat individu of de groep van individuen de bevoegdheid moeten hebben het algoritme te testen en/of de daaraan ten grondslag liggende beginselen te achterhalen. Dit haakt in op de verplichting ex artikel 15 AVG.

Op de derde plaats zouden er zorgspecifieke bigdatagovernancestructuren opgezet dienen te worden. Door partijen en experts uitgewerkte governanceregelingen kunnen een oplossing bieden voor het beter behartigen van de belangen van alle relevante belanghebbenden. Temeer omdat deze duidelijk toepasbare en, zeer belangrijk, controleerbare afspraken en geschillenregelingen kunnen bevatten.

Datagovernance houdt niet in '*one size fits all*'. Er zouden bigdatagovernancesystemen kunnen worden ontwikkeld voor vier te onderscheiden zorgdomeinen:

1. cure-care:
   a. zorgverlening;
   b. biomedisch wetenschappelijk onderzoek; en
   c. clinical trials;
2. zelfhulp/zelfzorg private sector (apps, PGDs/Quantified Self);
3. financieel (bekostiging en financiële afhandeling); en
4. maatschappelijke hulpverlening/publieke zorg (jeugd-, langdurige zorg, verplichte ggz en GGD).

Per domein kunnen partijen vervolgens, op basis van duidelijk gedefinieerde begrippen, afspraken maken en vastleggen in datagovernanceraamwerken. Prioriteit zou mijns inziens moeten liggen bij gegevensverwerkingen die het sterkst zijn gereguleerd, zoals die, die worden beheerst door de WGBO, Wbp, de Zvw en ook in het sociale domein/publieke zorg. Er dient daarbij per domein een 'tussenlaag' te worden gecreëerd die de principes, (grond)rechten en plichten uit de huidige formele wetgeving verbindt met de praktijk en toegesneden is op (de) technologische en maatschappelijke ontwikkelingen. Deze tussenlaag zal moeten bestaan uit toegesneden stelsels van afspraken, standaarden, codes en/of gecon-

cretiseerde, controleerbare en afdwingbare regelingen[57] die (per verwerking of groep van verwerkingen) steeds in een bepaalde context moeten worden geplaatst. Door middel van uitgebalanceerde datagovernancesystemen kunnen datastromen en techniek in goede en controleerbare banen worden geleid. Voortvarende samenwerking is geboden. 'Een voor allen, allen voor een'.[58]

57 Ook het advies van de RvZ uit 2014 (Consumenten eHealth) geeft deze oplossingsrichting. In zijn advies visualiseert de raad een mogelijk toekomstig neutraal stelsel van bindende afspraken en uniforme informatiestandaarden om te voorzien in adequate voorwaarden voor gegevensverwerking.

58 A. Dumas, *Les trois mousquetaires*, 1844.

Literatuur

Bovenberg (2006)
J.A. Bovenberg, *Property rights in blood, genes and data. Naturally yours* (diss. UL), Leiden/Boston, Martinus Nijhof Publishers, 2006.

Cate, Cullen, Mayer-Schönberger (2013)
F.H. Cate, P. Cullen, V. Mayer-Schönberger, *Data Protection Principles for the 21st Century, revising the OECD Guideline*, 2013.

Dobush (2013)
L. Dobush, *Algorithm Regulation #4: Algorithm as a Practice*, https://governancex-borders.com/2013/01/14/algorithm-regulation-4-algorithm-as-a-practice.

Dumas (1844)
A. Dumas, *Les trois mousquetaires,* 1844.

Institute for Health Technology Transformation (2013)
Transforming Health Care Through Big Data, Strategies for leveraging big data in health care industry, Institute for Health Technology Transformation, 2013.

Kranendonk (2013)
E.J. Kranendonk, 'Kind en biobank: enkele juridische aspecten', *TvGR* 2013. (37) 3.

Mikkers en Goudsmit (2016)
A. Mikkers en J. Goudsmit, 'Door algoritmes voorgerekende keuzes leiden tot foute beslissingen', *FD*, 30 november 2016.

Moerel (2014)
L. Moerel, *Big Data Protection, How to make the Draft EU Regulation Data Protection Future Proof*, Tilburg University, 2014.

Niessenbaum (2010)
H. Niessenbaum, *Privacy in Context, Technology, Policy and the Integrity of Social Life*, Stanford Law Books, 2010.

Ottes (2016)
L. Ottes, *Big data in de zorg*, Wetenschappelijke Raad voor het Regeringsbeleid, Den Haag, 2016.

Ploem (2010)
M.C. Ploem, 'Gegeven voor de wetenschap; Regulering van onderzoek met gegevens, lichaamsmateriaal en biobanken', in: *Wetenschappelijk onderzoek in de zorg*. Preadvies Vereniging voor Gezondheidsrecht, Den Haag, Sdu Uitgevers 2010.

Schönberger en Cukier (2013)
V. Mayer-Schönberger en K. Cukier, *De Big Data Revolutie*, Maven Publishing, 2013.

Stalder (2012)
F. Stalder, *Between Democracy and Spectacle. The Front and Back of the Social Web*, http://felix.openflows.com/node/223.

Warren en Brandeis (1890)
S. Warren en L. Brandeis, 'The Right to Privacy', *Harvard Law Review* 4 (5), 193-220, 1890.

Westin (1967)
A.F. Westin, *Privacy and Freedom*, New York 1967.

WRR (2016)
Big Data in een vrije en veilige samenleving, Wetenschappelijke Raad voor het Regeringsbeleid, Amsterdam University Press, 2016.

Deel 2
Controle en toezicht op gebruik van big data

Privacyrisico's en -waarborgen bij het gebruik van big data tegen zorgfraude: een verkenning

PROF. MR. G.J. ZWENNE EN MR. DR. DRS. W.A.M. STEENBRUGGEN

Deel 2
Controle en toezicht op gebruik van big data

Privacyrisico's en -waarborgen bij het gebruik van big data tegen zorgfraude: een verkenning

Prof. mr. G.J. Zwenne en mr. dr. drs. W.A.M. Steenbruggen*

* Gerrit-Jan Zwenne is hoogleraar recht en de informatiemaatschappij aan de Universiteit Leiden en advocaat en partner bij Brinkhof NV te Amsterdam. Wilfred Steenbruggen is advocaat in technologie, media en telecommunicatie (TMT) en gezondheidszorg & life sciences bij Leijnse Artz advocaten te Rotterdam.

1 Inleiding

Er is veel aandacht voor zorgfraude. In de landelijke media, zowel online als offline, zien we vrijwel dagelijks soms wat tendentieus of schreeuwerig getoonzette berichten, zoals dat 'artsen voor miljard euro frauderen',[1] 'miljoenenfraude in de thuiszorg',[2] 'zorgfraude ziekenhuizen voor tientallen miljoenen',[3] '2,5 miljoen boete voor St. Antonius Ziekenhuis wegens foute declaraties'[4] of meer anekdotisch 'tandartsrekening voor niet-bestaande cliënt,[5] 'rekening voor afgezegd consult',[6] 'Nijverdaller Wesseling krijgt dubbele rekening ziekenhuis',[7] 'frauderen blijkt een fluitje van een cent',[8] 'VVD wil frauderende pgb-bemiddelaars op zwarte lijst',[9] 'Opnieuw geknoei met declaraties in de ggz',[10] 'Zorgverzekeraars hebben geen idee welke psychische zorg zij vergoeden'[11] en 'Miljoenenverlies zorgverzekeraars door EuroPsyche'.[12]
Het voorgaande is een willekeurige greep uit de vele nieuwsberichten die ons in de laatste jaren hebben bereikt. We moeten daarbij natuurlijk onderkennen dat de keuze voor het taalgebruik in deze berichten en de redactie van de koppen erboven, ook verband houden met de commerciële wens om meer lezers te bereiken en meer clicks te genereren. En ook dat het helemaal niet is gezegd dat in al deze gevallen ook daadwerkelijk sprake is van opzettelijk frauduleus handelen. Toch maakt het wel duidelijk dat er het nodige misgaat bij het declareren door zorgaanbieders en dat daarmee grote bedragen zijn gemoeid. Hoe groot precies is niet bekend. Schattingen lopen uiteen van tientallen miljoenen euro's tot enkele miljarden euro's per jaar.[13]
Dit soort bedragen zet de betaalbaarheid van ons zorgstelsel onder druk en leidt tot erosie van solidariteit, zeker in tijden waarin de zorgkosten toch al sterk oplo-

---

1 Nu.nl 4 november 2011 www.nu.nl/economie/2659067/artsen-frauderen-miljard-euro.html.
2 Een vandaag 12 juni 2009 www.eenvandaag.nl/binnenland/34816/miljoenenfraude_in_de_thuiszorg.
3 Nu.nl 16 mei 2013 www.nu.nl/binnenland/3476441/zorgfraude-ziekenhuizen-tientallen-miljoenen.html.
4 Nu.nl 11 februari 2014 www.nu.nl/economie/3698935/25-miljoen-boete-st-antonius-ziekenhuis.html.
5 *NRC* 4 september 2013.
6 *Tubantia* 12 augustus 2014.
7 *Tubantia* 1 augustus 2014.
8 *AD* 14 februari 2013.
9 Nu.nl i juli 2015 www.nu.nl/politiek/4079090/vvd-wil-frauderende-pgb-bemiddelaars-zwarte-lijst.html.
10 Nos.nl 27 december 2015 http://nos.nl/artikel/2077357-opnieuw-geknoei-met-declaraties-in-de-ggz.html.
11 *Volkskrant* 4 mei 2012.
12 *Volkskrant* 14 februari 2013.
13 PWC (2013), *Naar een fraudebeeld Nederland*.

pen door de vergrijzing. Het verbaast dan ook niet dat wordt aangedrongen op een stevige aanpak van zorgfraude. Met name vanaf 2011 wordt er hard geroepen om handhaving en *naming and shaming* van 'sjoemelende zorginstellingen, frauderende ziekenhuizen en malafide pgb-bemiddelingsbureaus'. Daarbij wordt veel verwacht van de inzet van big data. In de zorgsector worden enorme hoeveelheden gegevens verzameld en bij elkaar gebracht, bij zorgverzekeraars en bij toezichthouders. Deze gegevens zouden met behulp van slimme data-analyses (*big data predictive analytics*) mogelijk onregelmatigheden en fraude sneller en beter kunnen herkennen, zodat deze kan worden voorkomen of in elk geval dat daartegen kan worden opgetreden.
Voor de meeste juristen en vele anderen is het thema big data onlosmakelijk verbonden met vragen over privacy- en gegevensbescherming. Onbegrijpelijk is dat niet. Als het gaat om big data zijn er wel meer belangrijke rechtsvragen, bijvoorbeeld op het gebied van intellectuele eigendom,[14] mededingingsrecht[15] of consumentenbescherming,[16] maar de op dit moment meest urgente vragen, althans de vragen waarover de grootste zorgen zijn, hebben vooral betrekking op de risico's ervan in termen van bedreigingen van de persoonlijke levenssfeer en de bescherming van persoonsgegevens. Deze vragen zijn ook pregnant aanwezig bij de inzet van big data in de context van de bestrijding van zorgfraude, zeker indien gezondheidsgegevens bij de analyse worden betrokken.
In deze bijdrage hebben wij er daarom voor gekozen om het gebruik van big data in het kader van het tegengaan van zorgfraude vooral vanuit het perspectief van privacy- en gegevensbescherming te bezien. Eerst beschrijven we op welke wijze nu al gebruik wordt gemaakt van data-analyses om zorgfraude tegen te gaan (par. 2). Vervolgens gaan we in op de risico's die we daarbij zien (par. 3), waarna we bij wijze van vingeroefening enkele waarborgen bespreken waarin wet- en regelgeving voorziet om de verschillende rechtssubjecten (zoals verzekeringnemers en verzekerden, patiënten, zorgaanbieders etc.) te beschermen (par. 4). We sluiten af met een korte beschouwing over de vraag of dat genoeg is (par. 5).

14 Bijv. B. Lundqvist, (2016). *Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet of Things World*, Faculty of Law, University of Stockholm Research Paper No. 1. https://ssrn.com/abstract=2891484.

15 Zie bijv. W. Kerber, (2016). *Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection*, MAGKS, Joint Discussion Paper Series in Economics, No. 14-2016. https://ssrn.com/abstract=2770479.

16 Bijv. M. Rhoen, M., (2015). Big Data and Consumer Participation in Privacy Contracts: Deciding who Decides on Privacy. *Utrecht Journal of International and European Law* 31(80), p. 51–71. DOI: http://doi.org/10.5334/ujiel.cu.

2 Bestrijding van zorgfraude door middel van (big)data-analyses

2.1 Aanloop

Fraude is van alle tijden, ook in de zorg.[17] De invoering van het nieuwe zorgstelsel in 2006 leidde evenwel tot een hernieuwde aandacht voor het onderwerp. In de aanloop daarheen werd duidelijk dat er niet alleen frauderisico's zijn aan de zijde van de zorgvrager, maar ook aan de zijde van de zorgaanbieders.[18] En daarbij speelt vooral de aard van het bekostigingssysteem een belangrijke rol. Hoe complexer namelijk de tarieven zijn, hoe groter de risico's op fouten en fraude aan de kant van de zorgaanbieder.[19] En dat het systeem van prestatiebekostiging op basis van diagnose-behandelcombinaties (DBC's) complex is, behoeft weinig betoog. Weliswaar is het DBC-systeem in 2012 aanzienlijk vereenvoudigd met de invoering van de DOT-methodiek (DBC's op weg naar transparantie) die het aantal zorgproducten en tarieven terugbracht van 30.000 naar zo'n 4.400, maar het is nog steeds erg ingewikkeld en dus foutgevoelig en daarmee fraudegevoelig.
Onder de Wet tarieven gezondheidszorg (Wtg)[20] werden er daarom al maatregelen genomen om fouten en fraude door zorgaanbieders te voorkomen, met name door de transparantie rondom prestatie en tarief te vergroten en het bestuursrechtelijk toezicht te verstevigen. Het wetsvoorstel WTG ExPres[21] voorzag bijvoorbeeld in algemene administratievoorschriften voor zorgaanbieders en verzekeraars, zodat deze gehouden zouden zijn om een administratie te voeren waarin niet alleen de geleverde prestaties zichtbaar zijn, maar ook de daarvoor in rekening gebrachte tarieven en de in verband daarmee ontvangen of verrichte betalingen en vergoedingen aan derden. Daarbij kwamen nieuwe verplichtingen ten aanzien van tijdige patiënteninformatie en de wijze waarop wordt gedeclareerd. Daarnaast werd er een centraal Meldpunt Onregelmatige Declaraties ingesteld bij de toezichthouder, indertijd het College tarieven gezondheidszorg (CTG). Ook kreeg het CTG meer mogelijkheden om informatie te vorderen (van een ieder) en uit te wisselen met andere toezichthouders en kon hij voortaan een last onder bestuursdwang of een last onder dwangsom opleggen bij overtreding van deze administratie-, declaratie- en informatieverplichtingen.

---

17 Zie uitgebreid T.A.M. van der Ende, 'Zorgfraude: van handhaving en hoe systemen hun eigen ongelukken creëren', in: J.G. Sijmons e.a., *Op weg naar 10 jaar nieuw zorgstelsel: terug- en vooruitblik*, Den Haag: Sdu Uitgevers 2015, p. 174 e.v.

18 *Kamerstukken II* 2002–2003, 28 828, nr. 1 en bijlagen.

19 Vgl. ook Van der Ende 2015, p. 188.

20 Wet van 20 november 1980, houdende regelen met betrekking tot de tarieven van organen voor gezondheidszorg, *Stb*. 1980, 646 (ingetrokken *Stb.* 2006, 415).

21 *Kamerstukken II* 2003/2004, 29379, nrs. 1-2.

In de Wet marktordening gezondheidszorg (Wmg[22]) is ingezet op een verdere versteviging van het bestuursrechtelijk toezicht op zorgverzekeraars en zorgaanbieders. Onder de Wtg kon het CTG niet punitief optreden tegen een overtreding van artikel 2 Wtg op grond waarvan zorgaanbieders geen tarieven voor prestaties in rekening mogen brengen die afwijken van of hoger zijn dan het gereguleerde tarief. Opzettelijke overtredingen waren echter wel via de band van de Wet economische delicten (Wed) strafrechtelijk gesanctioneerd. De rechtsopvolger van het CTG, de Nederlandse Zorgautoriteit (NZa), kan echter wel (forse) bestuurlijke boetes opleggen, tot maximaal € 500.000 of, als dat meer is, tot maximaal 10 procent van de omzet van de onderneming in Nederland, ook bij overtreding van artikel 35 Wmg dat – net als voorheen artikel 2 Wtg – zorgaanbieders verbiedt om tarieven in rekening te brengen die in strijd zijn met de tarief- of prestatieregulering, en zorgverzekeraars om die tarieven te betalen. Voor zware gevallen van fraude is strafrechtelijke sanctionering mogelijk gebleven.[23]
Desondanks kwam de fraudebestrijding in de zorg in de eerste jaren na invoering van het nieuwe zorgstelsel nog niet echt van de grond. Wij kunnen slechts speculeren over de oorzaken, maar het lijkt erop dat de transitie naar het nieuwe en complexe zorgstelsel gewoon veel tijd vergde – tijd die de stakeholders (politiek, toezichthouders en veldpartijen) nodig hadden om uit te vinden wat precies de juiste invulling van hun rol moet zijn binnen het nieuwe stelsel, ook ten opzichte van andere partijen. Misschien koos de NZa daarom aanvankelijk ook wel voor een 'zachtere' toezichtsstijl waarbij de nadruk vooral op informeel en preventief toezicht lag (door middel van informatieverzoeken en zogenaamde 'wenkbrauwgesprekken').
Van het gericht opsporen van fraude en repressief optreden door de NZa was in die eerste jaren in ieder geval geen sprake. Bij de eerste evaluatie van de Wmg in 2009 werd zelfs de vraag opgeworpen of de NZa die omslag naar meer repressief toezicht wel zou kunnen maken.[24] Inmiddels is duidelijk geworden dat de NZa wel degelijk repressief *kan* optreden: in de afgelopen jaren heeft de NZa een aantal malen forse boetes opgelegd aan zorgaanbieders in verband met onjuist declareren.[25] Dit laat onverlet dat de NZa nog steeds terughoudend lijkt bij de inzet van het boete-instrument. Het aantal boetes sinds de invoering van het nieuwe zorgstelsel is nog steeds op twee handen te tellen: sinds 2011 heeft de NZa nog maar acht boetes opgelegd. Dat is erg weinig als wordt gekeken naar vele on-

22 Wet van 7 juli 2006, houdende regels inzake marktordening, doelmatigheid en beheerste kostenontwikkeling op het gebied van de gezondheidszorg (Wet marktordening gezondheidszorg), *Stb.* 2006, 415.
23 *Kamerstukken II* 2004/05, 30186, nr. 3, p. 25.
24 Zie R.D. Friele e.a., *Evaluatie Wet Marktordening Gezondheidszorg*, Den Haag: ZonMw 2009, p. 147 e.v.
25 Zo kreeg de Ommelander Ziekenhuis Groep wegens niet correct declareren in 2011 een boete van € 500.000, het St. Antonius Ziekenhuis in 2014 een boete van € 2.500.000 en Stichting Altrecht in 2015 een boete van € 700.000.

regelmatigheden en daarmee gemoeide miljardenbedragen die de afgelopen jaren zijn langsgekomen onder de noemer fraude in de zorg.
Mede daardoor staat, met name sinds 2013, de bestrijding van zorgfraude hoog op de politieke agenda. Zorgaanbieders, zorgverzekeraars en handhavingspartners hebben, op aandringen van het parlement, allerlei initiatieven genomen en samenwerkingsverbanden opgezet om de kwaliteit van declaraties te vergroten en fouten en fraude te voorkomen. Ook wordt ingezet op een meer integrale handhaving en nauwe samenwerking van handhavingspartners bij de opsporing en vervolging van onrechtmatigheden. Deze (publiek-private) samenwerking vormt de opmaat tot verder gezamenlijk gebruik van databestanden voor fraudebestrijding. Zowel in geval van verdenkingen als voor het analyseren van risico's vanuit grote hoeveelheden data.

2.2 Big data en fraudebestrijding

De term big data wordt in veel verschillende betekenissen gebruikt.[26] De gemeenschappelijke deler is dat het gaat om het verzamelen en gebruiken van grote volumes data afkomstig uit diverse bronnen die niet altijd eenvoudig doorzoekbaar of koppelbaar zijn. De desbetreffende gegevensverzamelingen laten zich hierdoor lastig gericht, op basis van vooraf opgestelde hypotheses en vraagstellingen, doorzoeken. Daarom wordt met complexe zoekalgoritmes gezocht naar mogelijk interessante verbanden en patronen in de data. Dit kan leiden tot nieuwe en soms volstrekt onverwachte inzichten die kunnen worden gebruikt voor het opstellen van risico- en andersoortige profielen.
In de private sector kennen we verschillende voorbeelden van organisaties die op basis van aankoopgegevens of gegevens over wat wij doen op internet (surfgedrag) klant- of gebruikersprofielen opstellen aan de hand waarvan ze vervolgens gerichte aanbiedingen kunnen doen ('behavorial advertizing' of 'behavorial targeting').[27] Al wat langer kennen we de risicoprofielen met betrekking tot kredietwaardigheid en betalingsgedrag ('credit score') op basis waarvan wordt bepaald of klanten al dan niet in aanmerking komen voor een krediet of voor een bepaalde betaalwijze (denk aan: kopen op afbetaling). Van sommige vliegmaatschappijen wordt wel gezegd dat op basis van dergelijke profielen de door een klant te betalen ticketprijs wordt gepersonaliseerd, wat naar verluidt met zich kan brengen

26 Zie voor een overzicht WRR, *Big data in een vrije en veilige samenleving*, Amsterdam: Amsterdam University Press 2016, p. 33 e.v. en hoofdstuk 1a van dit preadvies.

27 Zo kon de Amerikaanse supermarkt Target aan de hand van een dergelijke analyse voorspellen of iemand zwanger was en daarop inspelen door aanbiedingen. Zie C. Duhigg, 'How Companies Learn Your Secrets', *New York Times* 16 februari 2012. Zie ook uitgebreid over behavioral targeting: F. Zuiderveen Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting*, Deventer: Kluwer Law International 2015.

dat de gebruikers van dure computers (zeg: een Apple Macbook) een hogere prijs betalen dan degenen die gebruikmaken van een goedkopere Windows-pc.[28]
Ook in de publieke sector zijn tal van voorbeelden te vinden van het gebruik van big data. Vaak wordt daarbij direct gedacht aan de onthullingen van Snowden over de Amerikaanse veiligheidsdienst NSA die op ongekend grote schaal data verzamelt over het wereldwijde telecommunicatie- en internetgebruik, maar ook in Nederland wordt al gebruikgemaakt van data-analyses en profilering. Zo maakt de Belastingdienst bijvoorbeeld al veelvuldig gebruik van bigdata-analyses om belastingfraude te kunnen opsporen,[29] de politie gebruikt data-analyses om criminele hotspots en veelplegers te vinden om preventief misdaad te bestrijden,[30] gemeenten, UWV en andere instanties maken gebruik van het Systeem Risico Indicatie (SyRI) om risicoanalyses uit te voeren met het oog op de opsporing van socialezekerheidsfraude,[31] de marechaussee kijkt naar opvallende reisbewegingen van voertuigen of personen en financiële toezichthouders kijken naar afwijkende transacties, boven een bepaald bedrag of naar een bepaald land, om te bepalen hoe en waar zij hun toezichtsbevoegdheden inzetten.[32]
Als het gaat om fraudebestrijding betekent het gebruik van big data vooral het kunnen voorspellen welke patronen (zoals combinaties van eigenschappen en kenmerken van personen, gedragingen, geldstromen etc.) naar verwachting aanduiden waar de grootste statistische kans is dat er sprake is van fraude of onregelmatigheden. Dit kan samengaan met profilering van situaties en personen. Het is de fraudebestrijders echter niet zozeer te doen om het vinden van patronen – dat is een tussenstap – maar om het zo snel mogelijk in beeld brengen van fraudeurs op naam. Het gaat hun om het in beeld brengen van concrete frauderisico's, het vergroten van pakkansen van fraudeurs en uiteindelijk het identificeren van de fraudeurs, zodat die daadwerkelijk 'gepakt' kunnen worden. Voor het oplossen van concrete zaken wordt dan ook niet alleen gebruikgemaakt van grote databestanden (big data). Veel vaker is sprake van analyse van een relatief beperkte set data over een persoon of zaak (little data), veelal al met een min of meer concrete verdenking.

---

28 J. Angwin & D. Mattioli, 'Coming Soon: Toilet Paper Priced Like Airline Tickets', *Wall Street Journal* 2 september 2012. Over personalised pricing zie ook OFT, *Personalised Pricing*, May 2013, OFT 1489.

29 P. Olsthoorn, *Big Data voor Fraudebestrijding*, WRR: Den Haag 2016.

30 Zie D. Willems & R. Doelemans, 'Predictive Policing – wens of werkelijkheid?', *Tijdschrift voor de Politie*, 2014-4/5, p. 39 e.v.

31 Olsthoorn 2016, p. 99 e.v.; zie over SyRI ook G-J. Zwenne & A.H.J. Schmidt, 'Wordt de homo digitalis bestuursrechtelijk beschermd?', in: *Homo Digitalis*, NJV-preadvies 2016; Deventer 2016, p. 310 en 339-341.

32 B.H. Custers, 'Risicogericht toezicht, profiling en Big Data', *Tijdschrift voor Toezicht* 2014/5, p. 9-16.

2.3 Voorbeelden van (big)data-analyse bij de aanpak van zorgfraude

Fraudebestrijding door middel van data-analyse is in de zorg nog een relatief nieuw fenomeen. De meeste gevallen van fraude komen nog steeds aan het licht door middel van tips, bijvoorbeeld van patiënten die een factuur zien en vaststellen dat de gefactureerde behandeling niet overeenkomt met de ondergane behandeling en dit melden bij hun zorgverzekeraar of de NZa. Maar dat laat onverlet dat er al wel degelijk gebruik wordt gemaakt van data-analyse en patroonherkenning bij de bestrijding van zorgfraude. Dit zal naar verwachting in de toekomst alleen maar verder toenemen.
We bespreken niet-uitputtend een aantal voorbeelden van data-analyse bij de bestrijding van zorgfraude. Daaruit blijkt niet alleen dat big data ook wat betreft de bestrijding van zorgfraude veel potentie heeft. De voorbeelden maken vooral duidelijk dat, zeker in samenwerkingsverbanden, de succesvolle inzet van big data bij de bestrijding van zorgfraude in de praktijk nog niet zo eenvoudig is. En dat is eigenlijk ook wel het meer algemene beeld bij gegevensuitwisseling en data-analyse in de toezichts- en handhavingspraktijk. Hiervan wordt, niet ten onrechte, veel verwacht, maar in de praktijk blijkt deze gegevensuitwisseling en data-analyse dusdanig omgeven met lastige technische, organisatorische en juridische vraagstukken dat deze in het geheel niet van de grond komt of, als dat wel het geval is, niet voldoet aan de verwachtingen.
Dat blijkt bijvoorbeeld ook uit de gang van zaken rondom het Expertisecentrum Zorgfraudebestrijding (EZB). Dit EZB is in 2013 opgericht door de Taskforce Integriteit Zorgsector (TIZ) ter uitvoering van het convenant ter verbetering van de bestrijding van zorgfraude tussen de NZa, IGZ, Zorgverzekeraars Nederland, Centrum Indicatiestelling Zorg (CIZ), Inspectie SZW, FIOD, Belastingdienst en OM. Het convenant is tot stand gekomen onder regie van VWS en heeft tot doel de samenwerking in de keten te verbeteren bij de aanpak van zorgfraude, met name door meer informatie-uitwisseling (waaronder persoonsgegevens) over ernstige zorgfraudes en gezamenlijk gebruik van databestanden voor zover mogelijk binnen de wettelijke kaders. Daarnaast voorzag het convenant in de oprichting van projectorganisatie en werkgroepen voor 'specifieke risicoanalyse'.[33] Hiervoor werd in 2013 het EZB opgericht, in eerste instantie bij wijze van pilot.
Het EZB had zowel een strategische als operationele functie. De operationele functie omvatte de centrale aanpak van meervoudige zorgfraudezaken op terreinen waar de grootste risico's liggen. Bij de strategische functie ging het om het maken van analyses met het doel om meer zicht te krijgen op waar zorgfraude vooral speelt en hoe dat te herkennen. Intelligence speelde daarbij een grote rol. Het was expliciet de bedoeling om gegevens uit bestaande grote databases, zoals de Vektis-database en het DBC-informatiesysteem (DIS), te koppelen en door middel van bestandsanalyse patronen te zoeken die een aanwijzing zouden opleveren voor frauduleus handelen. Vektis beheert als uitvoeringsorganisatie van

33 *Kamerstukken II* 2012/2013, 28828, nr. 50.

zorgverzekeraars een omvangrijke database met de declaratiegegevens van nagenoeg alle zorgverzekeraars.[34] En het DIS, dat inmiddels is ondergebracht bij de NZa, bevat alle gegevens van zorgaanbieders over afgesloten DBC-trajecten in de ziekenhuiszorg, ggz en forensische zorg en over trajecten in de basis-ggz.[35] Ook zou het EZB gevoed worden met fraudesignalen vanuit het Verzamelpunt Zorgfraude dat ook op grond van het al genoemde convenant was ingesteld.
Dit klinkt allemaal dus al wel echt als big data. Er werd dan ook veel van het EZB verwacht. In de praktijk bleek het echter geen succes. Volgens Olsthoorn, die daarbij een woordvoerder van de NZa aanhaalt, werkte het in de vorm van het experiment niet. 'Vooral de algemene analyses waren niet goed genoeg om te worden toegepast.'[36] In 2015 is het EZB dan ook een stille dood gestorven.
Zorgverzekeraars zijn daarnaast ook al enige tijd bezig met data-analyses in de strijd tegen zorgfraude. Zij zijn wettelijk verplicht na te gaan of ingediende declaraties voor vergoeding in aanmerking komen en moeten in dat verband controleren of 1) patiënten verzekerd zijn voor geleverde zorg en of gehanteerde tarieven kloppen (formele controle)[37] en 2) of door de zorgaanbieder in rekening gebrachte zorg ook daadwerkelijk is geleverd en het meest was aangewezen in het licht van de gezondheidstoestand van de patiënt (materiële controle).[38] Om dit effectief te kunnen doen, hebben zorgverzekeraars in de afgelopen jaren elk apart veel geïnvesteerd in de verbetering van hun processen en systemen voor controles en fraudebeheersing. Data-analyse door patroonherkenning speelt daarin een steeds belangrijkere rol om (risico's op) onrechtmatigheden te detecteren.[39]
Deze investeringen hebben ook wat opgeleverd. Uit cijfers van het Kenniscentrum Fraudebeheersing in de Zorg (onderdeel van Zorgverzekeraars Nederland) blijkt bijvoorbeeld dat zorgverzekeraars in 2014 2 miljard aan declaraties hebben afgewezen bij controle voor betaling (formele controle voor betaling). 449 miljoen euro is teruggevorderd door betaalde declaraties achteraf te controleren (formele controles na betaling en materiële controles). Er is voor 18,7 miljoen euro aan fraude geconstateerd.[40] En in 2015 is bij controle voor betaling voor een bedrag van 2,4 miljard euro aan declaraties door zorgverzekeraars afgewezen. Via controles na betaling is er 485 miljoen euro teruggevorderd. In 2015 is er voor 11,1 miljoen euro aan fraude vastgesteld.[41]

---

34 Zie www.vektis.nl
35 Zie dbcinformatiesysteem.nl.
36 Olsthoorn 2016, p. 37.
37 Art. 1, aanhef, en onder t, Regeling zorgverzekering (Rzv).
38 Art. 1, aanhef, en onder u, Rzv.
39 Zo beschikt bijv. Achmea al sinds 2011 over een eigen Kenniscentrum voor onderzoek en analyse van de data in haar eigen Achmea Health database. Dit Kenniscentrum doet niet alleen onderzoek met het oog op fraudebestrijding, maar ook met het oog op de verbetering van zorginkoop of -verlening. Zie Olsthoorn 2016 p. 46 e.v.
40 Zorgverzekeraars Nederland, *Rapportage controle en fraude 2014* www.zn.nl.
41 Zorgverzekeraars Nederland, *Rapportage controle en fraude 2015* www.zn.nl.

De cijfers maken echter ook duidelijk dat er een groot verschil in omvang bestaat tussen fouten en fraude. Het bedrag aan geconstateerde fraude bedraagt minder dan 1 procent van het totale bedrag aan onjuist geachte declaraties. Dat wil niet per se zeggen dat het dus met de fraude in de zorg wel meevalt. Fraude is een heftige beschuldiging en moet dus zorgvuldig worden onderbouwd. Juist omdat nu eenmaal veel fouten worden gemaakt en vaak lastig te achterhalen is of de boel bewust wordt geflest, zijn zorgverzekeraars terughoudend met de kwalificatie fraude en kiezen zij er veelal voor om hun geld terug te vorderen, desnoods via de rechter,[42] en eventueel om het contract met een bepaalde zorgaanbieder te beëindigen.[43] Het lijkt dan ook aannemelijk dat veel gevallen waarin sprake is van fraude niet worden opgepikt en (tucht-, bestuurs- of strafrechtelijk) vervolgd, omdat niet bewezen kan worden dat sprake is van fraude of het daarmee gemoeide belang eenvoudig te gering is en de kosten dus niet tegen de baten opwegen.
Het is goed mogelijk dat meer fraudegevallen zouden kunnen worden aangetoond, indien zorgverzekeraars nauwer zouden samenwerken en gebruik zouden maken van elkaars data en analyses. De NZa en de politiek willen ook graag dat zorgverzekeraars meer samen optrekken bij de bestrijding van fraude. Van gezamenlijk fraudeonderzoek door zorgverzekeraars is tot nog toe echter geen sprake. Het al genoemde Kenniscentrum Fraudebeheersing in de Zorg doet niet aan data-analyse, maar rapporteert enkel over de fraudemeldingen van de afzonderlijke verzekeraars. Wel hebben de zorgverzekeraars in 2015 aangegeven dat zij de mogelijkheden zullen verkennen om gezamenlijk fraudeonderzoek te doen door middel van een onafhankelijke, gezamenlijke onderzoeksunit.[44] Volgens Olsthoorn heeft gezamenlijk fraudeonderzoek voor een aantal grote zorgverzekeraars echter geen prioriteit, omdat zij de kostenbesparingen als gevolg van fraudebestrijding als concurrentievoordeel zien.[45]
Ook de NZa houdt zich bezig met big data, samen met handhavingspartners en veldpartijen (vgl. het reeds genoemde EZB), maar ook op eigen initiatief. Zo heeft de NZa, op verzoek van VWS, in 2013 en 2014 uitgebreid onderzoek verricht en laten verrichten om zicht te krijgen op de aard en omvang van onregelmatigheden in een aantal verschillende zorgsegmenten (huisartsen, mondzorg, farmacie, ggz, paramedische zorg en de medisch specialistische zorg).
In de eerste plaats heeft het Fraude Detectie Expertise Centrum (FDEC) in opdracht van de NZa met behulp van datamining een enorme hoeveelheid declaratiebestanden van zorgverzekeraars, zorgkantoren, CAK en CIZ (verzameld en aangeleverd door het reeds eerder genoemde Vektis) doorgelicht op zoek naar onre-

42 Zie bijv. Rb. Rotterdam Midden-Nederland 1 mei 2013, ECLI:NL:RBMNE:2013:BZ9057; Rb. Rotterdam 17 juli 2013, ECLI:NL:RBROT:2013:5587 en Rb. Midden-Nederland 9 juli 2014, ECLI:NL:RBMNE:2014:2742.
43 Olsthoorn 2016, p. 35.
44 Zorgverzekeraars Nederland, Plan van aanpak fraudebeheersing 2015-2017.
45 Olsthoorn 2016, p. 38.

gelmatigheden in declaraties. Voor deze analyse zijn 881 miljoen records gebruikt van declaraties van huisartsen, 190 miljoen records met betrekking tot mondzorg, 619 miljoen records met betrekking tot farmaceutische zorg, 4 miljoen records voor ggz-zorg, 166 miljoen voor paramedische zorg en 49 miljoen records voor medisch specialistische zorg. In totaal zijn maar liefst 1,9 miljard records die betrekking hebben op de jaren 2010-2012 door het FDEC geanalyseerd. Voor de ggz waren geen gegevens beschikbaar over 2012.
Het FDEC heeft op deze data een uitgebreide data-analyse gedaan om onregelmatigheden op te sporen in declaraties. Daarbij is in de eerste plaats gekeken naar harde overtredingen van declaratieregels en daarnaast naar opvallende afwijkingen ten opzichte van het gemiddelde declaratiegedrag (door het FDEC aangeduid als anomalieën).[46] Bij geconstateerde overtredingen is het daadwerkelijk vergoede bedrag vergeleken met het bedrag dat het volgens de declaratieregels zou moeten zijn. Bij anomalieën is het bedrag vergeleken met het bedrag dat hoort bij het gehanteerde referentiepunt.
Uit het onderzoek blijkt dat in de onderzochte zorgsegmenten de declaratieregels op grote schaal worden overtreden en/of sprake is van anomalieën. Die onregelmatigheden kunnen allerlei vormen aannemen, zoals ongeldige combinaties van declaraties, dubbele declaraties, upcoding, declaraties nadat de patiënt is overleden enzovoort. Het FDEC doet geen uitspraken over of in deze gevallen sprake is van frauduleus handelen, maar adviseert in deze gevallen nader onderzoek te doen om na te gaan of sprake is van oprechte vergissingen, opzet of dat de regels wellicht niet helder (genoeg) zijn. Het FDEC merkt daarnaast op dat ook de kwaliteit van de brongegevens in voorkomende gevallen een oorzaak kan voor het signaleren van merkwaardigheden.
Op basis van de gevonden overtredingen en anomalieën concludeert het FDEC dat in de onderzochte segmenten in 2010 minimaal een bedrag van 113 miljoen euro is gemoeid met onregelmatigheden en in 2011 minimaal 117 miljoen euro. Voor 2012 kon door het FDEC geen totaalcijfer worden gegeven, omdat over dat jaar ggz-gegevens ontbraken en bovendien ook de gegevens met betrekking tot de medisch specialistische zorg niet compleet waren.
De NZa heeft vervolgens ook nog zelf aanvullend onderzoek op basis van het DIS gedaan voor de ggz.[47] Dit onderzoek is uitgevoerd als aanvulling op de analyse van de declaratiegegevens voor de ggz, omdat de declaratiegegevens niet alle informatie bevatten die nodig is voor een volledige analyse. In het bijzonder is de daadwerkelijk bestede tijd (lees: geschreven tijd) niet bekend in de Vektisbestanden. In dit onderzoek heeft de NZa met name gekeken naar anomalieën op

46 Zie FDEC, *Onregelmatigheden in declaratiebestanden bij huisartsen, mondzorg, farmacie, GGZ, paramedische zorg en medisch specialistische zorg*, 28 augustus 2014. Beschikbaar via www.nza.nl.

47 NZa, *Tijdschrijven, verblijfsdagen en diagnoses in de GGZ. Een beeld van onregelmatigheden in de DIS data,* november 2014. Beschikbaar via www.nza.nl.

basis van de bestede tijd ten opzichte van de tijd die een zorgaanbieder gemiddeld besteedt aan een patiënt. Op basis van deze analyse heeft de NZa vastgesteld dat voor 2011 54,6 miljoen euro en in 2012 voor 50,8 miljoen euro te veel is uitbetaald. Ook heeft de NZa gekeken naar overlap in verblijfdagen. Op basis van deze analyse komt de NZa nog eens tot een te veel vergoed bedrag van 155 miljoen euro in 2012.
In haar eindrapport[48] is de NZa echter erg voorzichtig met het trekken van harde conclusies over zorgfraude op basis van deze onderzoeken, omdat de onderzochte bestanden niet voor het opsporen van fraude bedoeld zijn. De gegevens zijn niet altijd volledig en deels nog niet gecontroleerd door zorgverzekeraars. Wanneer ze wel zijn gecontroleerd en er correctie door de verzekeraar heeft plaatsgevonden, dan is de correctie niet altijd vastgelegd in de bestanden van Vektis. Ook voor de geconstateerde anomalieën geldt dat ze niet met zekerheid aan te merken zijn als een fout of fraude. Ze wijken weliswaar opvallend veel af van gemiddelden, maar daar kan in nader onderzoek een verklaring voor blijken te zijn. Andersom zijn overtredingen die niet afwijken, niet zichtbaar via deze methode. Spookzorg, het in rekening brengen van zorg die niet is geleverd, blijft bijvoorbeeld geheel buiten beeld, indien de declaraties geen fouten bevatten. De NZa geeft dan ook aan dat zij, de beperkingen van het onderzoek wegende, niet op een verantwoorde en betrouwbare wijze een totaalcijfer voor zorgfraude kan bepalen. Maar de analyse biedt naar het oordeel van de NZa wel inzicht in gevallen waar het mis kan zijn en geeft daarmee belangrijke input voor toezicht, nader onderzoek en mogelijkheden voor zorgverzekeraars om hun controleprocessen te verbeteren. Op grond hiervan beveelt de NZa dan ook onder meer aan dat zorgverzekeraars meer met data-analyse gaan doen om fraude te herkennen en aan te pakken.[49]

2.4 Wat brengt de toekomst?

Het doen van voorspellingen is lastig. Zeker als het om de toekomst gaat.[50] Maar afgaand op ontwikkelingen in andere domeinen is het meer dan aannemelijk dat er ook in het zorgdomein veel gebruik gaat worden gemaakt van data-analyse en big data. In de fiscale vakliteratuur worden bijvoorbeeld al methodes besproken gericht op het 'construeren van patronen op basis van (potentiële) toekomstige gedragingen' en het 'conceptualiseren van toekomstige non-compliante gedrags-

48 NZa, *Onderzoek naar kwetsbaarheden en financiële onregelmatigheden in de zorg*, november 2014. Beschikbaar via www.nza.nl.

49 Zie NZa, *Rapport Onderzoek zorgfraude: Tussenrapport (update)*, februari 2014, p. 13-17, 30-31, 38. Zie ook NZa, *Onderzoek naar kwetsbaarheden en financiële onregelmatigheden in de zorg*, november 2014. Beschikbaar via www.nza.nl.

50 De uitspraak 'prediction is very difficult, especially about the future' wordt wel toegeschreven aan Niels Bohr.

patronen'.[51] Ook in de toelichting bij het welbekende (beruchte) SyRI-besluit[52] wordt voorgesorteerd op scenario's die veel weg hebben van wat er in de scifi-speelfilm Minority Report wordt aangekondigd.[53]
Ook het buitenland biedt inzichten in wat er wellicht gaat komen. In de Verenigde Staten (waar anders) zien we dat Centers for Medicare and Medicaid Services (CMS), een federale verzekeringsorganisatie, data-analyses gebruikt om zorgfraude te voorkomen. Voorheen werden zorgdeclaraties digitaal en handmatig vergeleken met aangeleverde documentatie van de zorgprofessionals. Inmiddels vergelijkt het 'Fraude Prevention System' declaratiepatronen met profielen van fraudeurs. Zo worden de zorgaanbieders die meer uren declareren dan dat er in een dag passen eruit gepikt. En er wordt met behulp van gegevens uit sociale netwerken rekening gehouden met samenwerkingspartners van eerdere fraudeurs. Op deze manier worden naar verluidt honderden miljoenen dollars per jaar aan fraude opgespoord, significant meer dan de jaren voordat dit nieuwe systeem in werking werd gesteld.[54]
Bovenstaande praktijkvoorbeelden maken duidelijk dat dit ook voor ons geen ver-van-ons-bedshow is. Als het aan VWS en de NZa ligt, zal in de komende jaren in de strijd tegen zorgfraude steeds meer gebruik worden gemaakt van data-analyse en big data.[55] Door zorgverzekeraars in het kader van hun wettelijke controletaak, maar ook door de NZa en haar handhavingspartners in het kader van gericht toezicht en handhaving.

3 Beperkingen van, en risico's bij, gebruik van big data

Zorgverzekeraars en de NZa kunnen al beschikken over uitgebreide databases met heel veel gedetailleerde gegevens en hebben daarnaast uitgebreide wettelijke bevoegdheden om informatie op te vragen bij (onder meer) zorgaanbieders. Als deze gegevens naast elkaar gelegd worden en/of met andere bestanden (bijvoor-

51 T. van Berkhout & T. van Engers 'Onderzoeksmethodologie voor informatiegestuurd sociaal toezicht', *WFR* 2012/824.
52 Besluit van 1 september 2014 tot wijziging van het Besluit SUWI in verband met regels voor fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens met inzet van SyRI, *Stb*. 2014, 320.
53 Zwenne & Schmidt 2016, p. 339; Custers 2014.
54 Zie http://www.modernhealthcare.com/article/20160524/NEWS/160529960/commentary-medicares-big-data-tools-to-fight-and-prevent-fraud-yield; https://www.stopmedicarefraud.gov/fraud-rtc12142012.pdf.
55 Zie meer uitvoerig het Programmaplan Rechtmatige zorg en het Plan van aanpak Fouten en Fraude 2015-2018 (*Kamerstukken II* 2014/2015, 28828, nr. 29) dat in april 2015 door de minister van VWS aan de Kamer is aangeboden en de daaropvolgende voortgangsrapportages.

beeld die van de Belastingdienst of de Kamer van Koophandel) gekoppeld worden en door middel van geavanceerde technieken 'slim' geanalyseerd, kan dat inzichten opleveren op grond waarvan fouten en fraude veel gerichter en effectiever kunnen worden voorkomen, aangetoond en aangepakt. Daarmee kan in potentie heel veel geld worden bespaard en dat is relevant in deze tijden waarin de zorgkosten als gevolg van de vergrijzing een steeds groter beslag leggen op de publieke middelen. Toch is bij de inzet van big data ook terughoudendheid op zijn plaats. Ook big data kent namelijk zo zijn beperkingen en risico's.

3.1 Beperkingen van big data

Dat big data zo zijn beperkingen kent, blijkt bijvoorbeeld uit Google Flu Trends, een applicatie waarvan werd geclaimd dat die op basis van 45 zoektermen de opkomst van griepepidemieën realtime zou kunnen volgen en in kaart brengen. Ruim twee weken sneller dan de officiële overheidskanalen. Toch bleek Google Flu Trends de griep structureel te overschatten en miste de applicatie de buiten het winterseizoen optredende A-H1-N1-pandemie in 2009 volledig.[56]
Dit voorbeeld illustreert dat ook bij de analyse van grote hoeveelheden data de resultaten niet automatisch correct zijn. Maar er zijn nog andere beperkingen verbonden aan bigdata-analyses, zoals statistische tekortkomingen en beperkingen in het toepassingsbereik. Wij noemen de belangrijkste aandachtspunten bij het gebruik van big data.

3.1.1 Bias

In de eerste plaats is er het biasprobleem. Gegevens worden altijd in een specifieke context verzameld. Daardoor zit in bijna iedere dataset een specifieke bias. Als die niet wordt gecorrigeerd, kan dat makkelijk leiden tot onjuiste of anderszins problematische uitkomsten. Wanneer de politie bijvoorbeeld enkel in wijken met veel allochtonen ('mensen met een migrantenachtergrond') surveilleert, zullen politiedatabanken vooral gevuld zijn met juist dergelijke personen. En dat zal doorwerken in de gemodelleerde risicoprofielen die dan onevenredig veel van deze allochtonen bevatten. Vooral bij het combineren en hergebruiken van databronnen kan het lastig zijn om te achterhalen hoe de datasets tot stand zijn gekomen en wat dus de precieze bias is die in data zit.

56 D. Lazer, R. Kennedy, G. King en A. Vespignani, 2014, 'The Parable of Google Flu: Traps in Big Data Analysis,' *Science* 343 (6176): 1203–1205, beschikbaar op: https://dash.harvard.edu/bitstream/handle/1/12016836/The%20Parable%20of%20Google%20Flu%20(WP-Final).pdf?sequence=1.

3.1.2 Correlaties

Het is in de tweede plaats van belang te beseffen dat de verbanden die met behulp van bigdata-analyses worden gelegd, niet noodzakelijk causaal van aard zijn. Het gaat om correlaties, dat wil zeggen om statistische verbanden. En dat maakt dat het enkele feit dat iemand past binnen een profiel nog niet automatisch betekent dat hij dus ook het aan dat profiel gekoppelde gedrag vertoont. Het verband kan ook indirect zijn of zelfs berusten op louter toeval. Zonder een betrouwbare theoretische basis over het hoe en waarom van de gevonden correlaties en zonder goede aanwijzingen dat de verbanden causaal van aard zijn, kunnen daarop gebaseerde maatregelen de plank volledig misslaan. Het maakt daarbij nogal uit of de informatie enkel aanleiding is voor verder onderzoek of dat er hardere consequenties aan verbonden worden.

3.1.3 Foutmarges

In de derde plaats zijn profielen, en dat geldt ook voor profielen die zijn opgesteld op basis van *big data predictive analytics*, sowieso altijd een benadering van de werkelijkheid en bevatten zij dus foutmarges. Het gevaar bestaat daarmee dat op basis van profielen de verkeerde conclusies worden getrokken, bijvoorbeeld omdat ten onrechte wordt aangenomen dat iemand binnen het profiel valt (false positive) of dat ten onrechte wordt aangenomen dat iemand erbuiten valt (false negative). Dat sprake is van een foutmarge is voor het aanraden van een boek op Amazon of een film op Netflix niet erg. Maar het wordt wel problematisch als iemand op basis van analyses bijvoorbeeld ten onrechte op een no-flylist wordt gezet zoals de Amerikaanse senator Ted Kennedy[57] of Europees Parlementariër Sophie In 't Veld overkwam[58] of, in het kader van dit preadvies relevant, een zorgaanbieder ineens op een zwarte lijst van zorgverzekeraars komt en niet langer in aanmerking komt voor een bepaalde aanvullende verzekering.

3.1.4 Kwaliteit data

In de vierde plaats kan ook de data zelf onvolledig of onjuist zijn, met als gevolg dat ook de op basis daarvan bepaalde risicoprofielen onjuist kunnen zijn. Het FDEC en de NZa wijzen er in de door hen uitgevoerde analyses op de databestanden van Vektis niet voor niks op dat de onderzochte bestanden niet voor het opsporen van fraude bedoeld zijn en de gegevens niet altijd volledig zijn en deels nog niet gecontroleerd door zorgverzekeraars. Er is dan alle aanleiding voor voorzichtigheid met betrekking tot het trekken van harde conclusies. Het werken met

57 V. Mayer-Schonberger & K. Cukier, *Big data*, Boston: Mariner Books 2014, p. 166-167.

58 E. Nakashima, 'European Lawmaker To Sue U.S. Over Data', *Washington Post*, 1 juli 2008.

risicoprofielen vereist bovendien ook dat profielen voortdurend worden geactualiseerd. Profielen raken namelijk na verloop van tijd 'uitgewerkt', bijvoorbeeld omdat zorgaanbieders die aan het profiel voldoen, al zijn aangepakt of omdat de frauderende aanbieders hun gedrag aanpassen en daardoor buiten het profiel vallen.[59]

3.1.5 Incidenten

In de vijfde plaats is van belang te beseffen dat bigdata-analyses niet altijd de meest geschikte oplossing zijn voor een vraagstuk. Bigdata-analyses ontlenen hun waarde aan patroonherkenning in grote hoeveelheden data. Bigdata-analyses zijn dus vooral nuttig als er sprake is van een zekere regelmaat of in ieder geval bepaalde terugkerende kenmerken. Als iemand eenmalig of incidenteel een spooknota verstuurt, zal dat waarschijnlijk niet uit de bigdata-analyse blijken. Uiteraard is het wel mogelijk dat deze persoon dan op een andere manier tegen de lamp loopt, bijvoorbeeld omdat de betreffende 'patiënt' meldt dat hij geen zorg heeft genoten.

3.1.6 Afsluitend

Het voorgaande maakt duidelijk dat big data de nodige beperkingen kent die geadresseerd moeten worden indien wordt overwogen gebruik te maken van big data, zeker als daarop beslissingen worden gebaseerd die een serieus te nemen impact op personen hebben.
Een zorgvuldig gebruik van big data veronderstelt wat ons betreft dat zorgverzekeraars en toezichthouders die daarvan gebruik willen maken ervoor zorgen dat zij beschikken over de voor hun doeleinden benodigde gegevens en dat deze van voldoende kwaliteit zijn. Uiteraard zullen zij ook moeten beschikken over de nodige expertise om goede analyses uit te voeren en de uitkomsten op een passende en controleerbare wijze te duiden.
Een ander belangrijk aandachtspunt in dit verband wordt daarnaast gevormd door de beveiliging van de data. Met het verzamelen, opslaan, uitwisselen en koppelen van grote hoeveelheden data wordt de beveiliging daarvan steeds belangrijker. Ook goed beveiligde systemen kunnen worden aangevallen, door codes te kraken, hardware te manipuleren of anderszins de beveiliging te omzeilen. Dat het niet gaat om een theoretisch risico, blijkt wel uit de vele berichten over beveiligingsincidenten die bijna dagelijks in de media langskomen.[60] Naarmate de databestan-

59 Custers 2014, p. 12.

60 Zo berichtte Zembla in februari 2017 dat de Belastingdienst in de periode tussen 2013 en 2016 de beveiliging bij de zogenaamde Broedkamer, de data-analyseafdeling van de Belastingdienst, niet op orde had waardoor mogelijk onbevoegde personen binnen en buiten de fiscus toegang hebben gehad tot gevoelige gegevens waaronder persoonsgegevens. Zie http://zembla.vara.nl/nieuws/belastingdienst-overtreedt-willens-en-wetens-privacywet. De AP is inmiddels een onderzoek gestart.

den groter zijn en er meer partijen betrokken zijn bij de data-analyse en de gegevens gevoeliger zijn, neemt het belang van goede beveiligingsmaatregelen toe.

3.2 Risico's bij bigdata-analyses

Er is bovendien ook op meer principiële gronden aanleiding voor een terughoudend en zorgvuldig gebruik van big data, in zijn algemeenheid, maar ook zeker in de strijd tegen zorgfraude. In de literatuur wordt in dit verband een aantal risico's geïdentificeerd die geadresseerd moeten worden, wil het gebruik van big data maatschappelijk en juridisch aanvaardbaar zijn.[61]
Sommige van deze risico's vloeien voort uit het niet adequaat omgaan met een aantal van de bovengenoemde beperkingen. Andere risico's hebben te maken met de verzameling en analyse van grote hoeveelheden data die voor meerdere doeleinden worden gebruikt. Wij vatten de belangrijkste risico's samen.

3.2.1 Stigmatisering en discriminatie

Datagedreven oplossingen werken toe naar wat wel wordt aangeduid als *social sorting*, dat wil zeggen: het indelen van mensen in specifieke groepen of categorieën, waaraan in allerlei contexten een betekenis kan worden toegekend die niet altijd positief is. Bij big data gebeurt dat op basis van correlaties die in de data te vinden zijn. De afbakening van groepen op basis van big data kan evenwel problematisch zijn als de bias die in elke dataset zit, niet goed wordt geadresseerd. De conclusies kunnen dan niet perfect passen op de groep en leiden tot ongerechtvaardigde stigmatisering en discriminatie, met grote negatieve gevolgen voor individuen. Een voorbeeld is te vinden in een studie uit de VS waarin werd vastgesteld dat zoekacties met zogeheten 'black-identifying names' (bijv. 'Jermaine') aanleiding gaf tot webadvertenties gerelateerd aan 'arrest' terwijl zoekacties op 'white-identifying names' (zoals 'Geoffrey') heel andere, veel minder diskwalificerende resultaten opleverden. Waarom precies dit gebeurde, was onduidelijk. Wel was duidelijk dat er sprake was van onwenselijke 'racially biased results'.[62]

3.2.2 Blackbox en dehumanization

Het gaat hier om het ontbreken of wegvallen van de mogelijkheden (voor zowel degenen die beslissingen nemen als degenen die daardoor worden geraakt) om te begrijpen waarom beslissingen worden genomen. We denken dan vooral aan de situaties die worden beschreven in het werk van Kafka. Of, wat luchtiger, de sketch 'Computer Says No' uit de Britse comedy Little Britain, waarin iemand zich in een ziekenhuis moet verweren tegen een administratiesysteem dat een heel andere behandeling suggereert dan waarvoor de patiënt is gekomen.[63]

---

61 Zie uitvoerig WRR 2016, p. 88 e.v.
62 White House, *Big Data: Seizing Opportunities, Preserving Values*, May 2014, p. 7.
63 Een eenvoudige internetzoekactie op zoekwoorden <computer says no> en <little brittain> levert de vindplaats op van deze hilarische episode.

3.2.3 *Onschuldpresumptie en fair trial*

Bigdataprocessen kunnen daarnaast de onschuldpresumptie onder druk zetten en raken daarmee aan het recht op een eerlijk proces dat onder meer is gewaarborgd in artikel 6 EVRM.[64] Een aspect van de onschuldpresumptie is dat opsporingsbevoegdheden niet zomaar jegens eenieder mogen worden toegepast, maar dat er een redelijk vermoeden van het plegen van een strafbaar feit moet zijn of ten minste aanwijzingen voor de betrokkenheid bij strafbare feiten. Aan de verdachte komt bovendien een beschermde status toe om een eerlijk proces te waarborgen (denk aan het zwijgrecht en andere rechten die voortvloeien uit het nemo tenetur-beginsel, de inzage in processtukken en equality of arms). Degene die op basis van een data-analyse tot een risicogroep behoort die bijzondere aandacht krijgt, heeft die speciale status vaak (nog) niet en kan zich dus niet hiertegen verweren, als hij daarvan al op de hoogte is. Daarbij komt dat diegene ook vaak helemaal niet weet hoe de algoritmes, computersystemen en profielen werken, zodat een effectieve verdediging sowieso lastig is, ook nadat hij in een later stadium alsnog tot verdachte is 'gepromoveerd'. Dit maakt het eens te meer van belang dat zorgverzekeraars en toezichthouders zorgvuldig omgaan met big data en niet zomaar op basis daarvan overgaan tot het opleggen van sancties of andere ingrijpende maatregelen.

3.2.4 *Individuele en collectieve privacy*

De combinatie van volume en variëteit maakt dat bigdataprocessen drijven op een overvloed aan informatie die op verschillende manieren aan personen gekoppeld is of kan worden. Spanningen met privacy en het gegevensbeschermingsrecht zijn dan nooit ver. Het ongelimiteerd verzamelen, bijeenbrengen en hergebruiken van persoons- en andere gegevens, omdat die ooit wellicht van pas komen, staat op gespannen voet met kernprincipes van het gegevensbeschermingsrecht zoals gegevensminimalisatie en doelbinding, en proportionaliteit. Ook roept de mogelijkheid van heridentificatie van geanonimiseerde gegevens, bijvoorbeeld op basis van een koppeling van eigen data aan data uit heel andere bronnen, ook weer allerlei privacyvraagstukken op. Big data zet daarmee niet alleen de individuele privacy, maar ook – en met name – de collectieve privacy onder druk, dat wil zeggen: de waarde van privacy als collectief of maatschappelijk goed.

3.2.5 *De 'function creep' of 'mission creep'*

De term function creep ziet op het sluipenderwijs (op een zogenoemde glijdende schaal) uitbreiden of verbreden van de doeleinden waarvoor gegevens worden gebruikt. Soms is daarbij sprake van (al dan niet) voorziene of beoogde neven-

64 M. Hildebrandt, 'Data-gestuurde intelligentie in het strafrecht', in: *Homo Digitalis*, NJV-preadvies 2016; Deventer 2016, p. 188 e.v.

effecten. Zo is er sprake van function creep als videocameratoezicht eerst alleen werd ingezet voor het vergroten van de veiligheid in de openbare ruimte en vervolgens ook bruikbaar blijkt als opsporingsmiddel.[65] Een ander bekend voorbeeld betreft het geval waarin uit een data-analyse bleek dat gegevens betreffende onderwijsprestaties van kinderen (Cito-toets) een indicatie kunnen geven van problemen bij gezinnen die in aanmerking komen voor bemoeizorg.[66] Dat function creep geen theorie is, blijkt ook uit het gegeven dat de NZa voor haar onderzoek naar onregelmatigheden bij het declareren gebruik heeft gemaakt van Vektis-databestanden die daarvoor niet zijn bedoeld. Dat laat onverlet dat een bigdata-analyse op zo'n bestand nuttige inzichten kan opleveren, maar daarbij moet men zich wel realiseren dat het bestand voor een ander doel is aangelegd en er dus een bepaalde bias in kan zitten of relevante gegevens kunnen ontbreken.

3.3 Dus...

Het is niet gezegd dat al deze beperkingen en risico's altijd relevant zijn bij de inzet van big data in het kader van de strijd tegen zorgfraude, maar het maakt wel duidelijk dat er terughoudend en zorgvuldig te werk moet worden gegaan bij het gebruik van big data, zeker als daarop ingrijpende beslissingen worden gebaseerd. Er zijn dus waarborgen nodig en daarop gaan we in de volgende paragraaf in.

4 Welke waarborgen biedt privacy- en gegevensbeschermingswetgeving?

4.1 Aanloop

Het gebruik van big data in de strijd tegen zorgfraude kent dus de nodige haken en ogen. Dat maakt het van belang dat er een effectieve rechtsbescherming is tegen besluitvorming op basis van big data en risicoprofielen.
Afhankelijk van de specifieke situatie zijn er allerlei regels en normen waaraan rechtssubjecten rechtsbescherming kunnen ontlenen tegen de geschetste risico's. Als zorgtoezichthouders of gemeenten gezamenlijk hun gegevens gaan analyseren denken we aan de algemene zorgvuldigheidsnormen uit de Algemene wet bestuursrecht (Awb). Als het gaat om analyses door zorgaanbieders of -verzekeraars denken we aan contractuele en zorgvuldigheids- en betamelijkheidsnormen. Eerder nog denken we natuurlijk nog aan de fundamentele rechten en vrijheden, zoals vastgelegd in de Grondwet (GW), het Handvest voor de grondrech-

65 J.E.J. Prins, 'Function creep: over het wegen van risico's en kansen', in *Justitiële verkenningen: Function creep en privacy*, Boom: Den Haag 2011/8, p. 8 e.v.

66 Zie F. Kleeman, B. Gritter & J. Bouma, *Hoe preventiever, hoe liever!: Predictie en preventie van probleemgedrag bij 6/7-jarige kinderen in Coevorden*, RUG/Wetenschapswinkel april 2005, p. 18.

ten van de EU (HvEU) en de mensenrechtenverdragen (EVRM en IVBPR).[67] En bij het gebruik van big data gaat het dan vooral om het recht op bescherming van de persoonlijke levenssfeer (art. 10, eerste lid, GW, art. 7 HvEU, art. 8 EVRM, art. 17 IVBPR) en het daaraan verwante recht op bescherming van persoonsgegevens (art. 10, tweede lid GW, art. 8 HvEU). Als het gaat om data-analyses en big data komt evenwel ook (of: juist) veel betekenis toe aan de onschuldpresumptie (art. 48 HvEU, art. 6, tweede lid, EVRM, art. 14 IVBPR) en natuurlijk ook het discriminatieverbod (art. 1 GW, art 21 HvEU, art. 14 EVRM, art. 2 IVBPR).
Verder denken we vooral aan de wetgeving waaraan nadere regels worden gegeven ter bescherming van deze rechten en vrijheden, zoals dat voor het discriminatieverbod wordt gedaan in de Algemene wet gelijke behandeling en op termijn voor de onschuldpresumptie, zij het in de context van opsporing en vervolging, mogelijk in de wetgeving ter implementatie van de Onschuldpresumptierichtlijn.[68]
Verreweg het meest relevant voor big data, in elk geval het meest uitvoerig en gedetailleerd, zijn op dit moment evenwel de nadere regels die worden gesteld ter bescherming van het recht op bescherming van persoonsgegevens. Deze regels vinden we op dit moment in de Wet bescherming persoonsgegevens (Wbp) en straks, vanaf 25 mei 2018, in de Algemene Verordening Gegevensbescherming (AVG) in combinatie met de Uitvoeringswet AVG (Uw AVG).[69]
Voor de specifieke verhoudingen van zorgaanbieder en -afnemers zijn er natuurlijk ook wetten als de Wet op de geneeskundige behandelingsovereenkomst (art. 7:456 t/m 7:468 BW) en de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG) van belang. Echter, omdat we verwachten dat in deze verhoudingen (nog?) niet direct sprake zal zijn van data-analyses in het kader van de aanpak van zorgfraude, gaan we daarop in deze bijdrage niet verder in.[70] Ook kiezen we ervoor om voor dit moment nog even voorbij te gaan aan wetswijzigingen en wetsvoorstellen waarmee wordt beoogd de mogelijkheden om te komen tot een effectieve aanpak te verruimen. Dit omdat het, gelet op de heftigheid van de discussies daarover, nog te speculatief lijkt om op basis daarvan harde conclusies te trekken.

---

67 G.J. Zwenne & WA.M. Steenbruggen, 'Privacyvoorwaarden voor de iOverheid. Vuistregels voor wet- en regelgevers met betrekking tot overheidsinformatiesystemen', *Regelmaat* 2015/1, p. 19-36.

68 Zie ook: Proposal for a Directive of the European Parliament and of the Council on the strengthening of certain aspects of the presumption of innocence and of the right to be present at trial in criminal proceedings, 27.11.2013, COM (2013) 821 final.

69 Voor de aanpak van zorgfraude zal deze uitvoeringswet van belang zijn omdat daarin de regels voor het gebruik van gezondheidsgegevens te vinden zullen zijn.

70 Daarmee willen we niet zeggen dat de in deze verhoudingen verwerkte gezondheidsgegevens geen betekenis hebben in dergelijke analyses, maar waarschijnlijk eerder in relatie tot de in de privacy- en gegevensbeschermingswetgeving gestelde regels (zoals het doelbindingsvereiste).

Er is een duidelijke trend waarin de aanpak van zorgfraude door middel van (gezamenlijke) data-analyse meer aandacht krijgt en daarin zien wij een bevestiging dat big data veel meer betekenis zal krijgen en ook dat de beperkingen op het gebruik ervan niet zozeer in de zorgspecifieke wetgeving moeten worden gezocht, maar in de privacy- en gegevensbeschermingswetgeving. En daaruit dan vooral 1) de regels voor de verwerking van gezondheidsgegevens en 2) de doelbindingsvereisten, 3) de regels voor profilering en ten slotte 4) de transparantieverplichtingen, dat wil zeggen de verplichtingen om degenen over wie gegevens worden verwerkt (de zogenoemde betrokkenen of datasubjecten) daarover op begrijpelijke wijze te informeren. Voordat we komen tot enkele afsluitende woorden verkennen we, bij wijze van vingeroefening, de voor deze vier thema's gestelde regels en de daaruit voortvloeiende waarborgen.

4.2 Gezondheidsgegevens

De wetgever gaat uit van een ruim begrip van 'gegevens betreffende iemands gezondheid' of 'gezondheidsgegevens'. Eronder vallen niet alleen gegevens over ziektes, aandoeningen en stoornissen en de behandeling daarvan, maar ook het gegeven dat iemand ziek is zonder dat bekend is wat eraan mankeert.[71] Dit betekent dat een enkele ziekmelding of een ongespecificeerde tandartsrekening al onder het begrip kan vallen. En, hoewel vergezocht, is ook voorstelbaar dat onschuldige gegevens over geboortejaar of leeftijd, of woonplaats, kunnen worden opgevat als gezondheidsgegevens, aangezien ook dergelijke gegevens inzicht kunnen geven in de gezondheidstoestand van de betrokkene.[72]
Voor gezondheidsgegevens geldt een verwerkingsverbod. Op grond van artikel 16 Wbp respectievelijk artikel 9, eerste lid, AVG mogen dergelijke gegevens niet worden verwerkt (verzameld, vastgelegd, gebruikt etc.), tenzij sprake is van een *lex specialis* die dit wel uitdrukkelijk toestaat of als er gebruik kan worden gemaakt van een in de verordening of wet genoemde uitzondering. Deze uitzonderingen vinden we in artikel 21 Wbp en het daarmee overeenkomende artikel 23 UwAVG (ontwerp), en in artikel 23 Wbp respectievelijk artikel 9, tweede lid, onder a t/m j AVG. Van deze uitzonderingen biedt er naar onze indruk maar één duidelijk de ruimte om gezondheidsgegevens te verwerken in verband met een bigdata-analyse ten behoeve van de aanpak van zorgfraude.

---

71 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 109; Autoriteit persoonsgegevens, De zieke werknemer: beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers, z2015-00774, 23 februari 2016, p. 10; zie ook overw. 35 van de AVG.

72 Een hoge of lage leeftijd zegt immers iets over de kans om last te krijgen van bepaalde kinder- of ouderdomsziektes. En wie woont in Amsterdam of Utrecht heeft veel meer dan een inwoner van Zeeland of Drenthe een risico om klachten te krijgen door fijnstof.

En dat is de uitzondering van artikel 23, eerste lid, onder g, Wbp, die ziet op de gevallen waarin de gegevensverwerking nodig is met het oog op een zwaarwegend algemeen belang, waarbij er passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en dit bij wet wordt bepaald dan wel door de Autoriteit Persoonsgegevens ontheffing is verleend. Een voorwaarde die deze toezichthouder tegenwoordig[73] wel stelt aan het verlenen van zo een ontheffing is echter dat er reeds een wetsvoorstel aanhangig is waarin wordt voorzien in een wettelijke regeling die de verwerking mogelijk maakt.[74] Voor de verwerking van gezondheidsgegevens in het kader van de aanpak van zorgfraude lijkt een wettelijke regeling de enige echt goed begaanbare weg te zijn.

4.3 Doelbinding

Een belangrijk uitgangspunt uit de privacy- en gegevensbeschermingswetgeving is het doelbindings- of doelverenigbaarheidsvereiste. Dit verlangt enerzijds dat persoonsgegevens alleen mogen worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde verzameldoelen (art. 7 Wbp en art. 5, eerste lid, onder, b, AVG) en anderzijds dat deze gegevens, nadat ze zijn verzameld, alleen verder mogen worden verwerkt voor doeleinden die niet onverenigbaar zijn met de doeleinden waarvoor deze zijn verzameld (art. 9, eerste lid, Wbp en art. 5, eerste lid, onder, b, AVG). Of er sprake is van 'niet onverenigbaarheid' wordt bepaald aan de hand van de verwantschap tussen de onderscheiden doeleinden, de gevoeligheid van de gegevens, de gevolgen voor de betrokkenen en of de gegevens al dan niet van de betrokkenen zelf zijn verkregen, en de overige waarborgen die zijn getroffen ter bescherming van de betrokkenen. Daarbij komt veel betekenis toe aan de redelijke verwachtingen die de betrokkenen hebben met betrekking tot de verdere verwerking van hun gegevens (art. 9, tweede lid, Wbp, art. 6, vierde lid, AVG).[75]

---

73 Het beleid van de AP daarover is nog betrekkelijk onduidelijk. In de zaak die uiteindelijk leidde tot ABRvS 3 september 2008, ECLI:NL:RVS:2008:BE9698, AB 2008, 335, werd door de toezichthouder zelf betoogd dat een ontheffing ook kan worden verleend om een pilot mogelijk te maken, zodat aan de hand van de uitkomsten daarvan kan worden besloten om al dan niet zo'n wetsvoorstel voor te bereiden. In latere besluiten lijkt de toezichthouder daarvan afstand te hebben genomen, maar zonder uit te leggen wat de overwegingen daarvoor zijn.

74 In de context van een publiekrechtelijk samenwerkingsverband kunnen gezondheidsgegevens op grond van art. 22, vijfde en zesde lid, Wbp 'meeliften' met de verwerking van strafrechtelijke gegevens die nodig is om de publiekrechtelijke taken van de deelnemers aan dat samenwerkingsverband uit te voeren. Daarvan kan dan wellicht gebruik worden gemaakt door toezichthouders, zoals NZa en IGZ, en organen als de FIOD of gemeenten, maar niet door zorgverzekeraars en zorgaanbieders.

75 Zie overw. 50 AVG.

Deze doelverenigbaarheidsvereisten komen in verschillende andere gedaanten terug in de wetgeving. We zien het onder andere in het zogenoemde opslagbeperkingsvereiste dat verlangt dat gegevens niet langer worden bewaard dan nodig voor het doel waarvoor deze zijn verzameld (art. 10 Wbp, art. 5, eerste lid, onder e, AVG) en in het gegevensminimalisatiebeginsel, op grond waarvan niet meer gegevens mogen worden verzameld en verwerkt dan nodig voor het doel waarvoor deze zijn verzameld (art. 11, eerste lid, Wbp, art. 5, eerste lid, onder a, AVG).
Voor het doelbindingsvereiste in het algemeen, en voor het opslagbeperkings- en gegevensminimalisatievereiste in het bijzonder, is wel duidelijk dat er op zijn minst sprake is van een gespannen verhouding met de toepassing van bigdata-analyses. Vanuit het perspectief van big data ligt het voor de hand om zoveel mogelijk gegevens zolang mogelijk te bewaren – wie weet levert het nog bruikbare correlaties, patronen en trends op – terwijl deze gegevensbeschermingsvereisten juist erop zijn gericht om over zo min mogelijk gegevens te beschikken. Als zodanig lijken deze vereisten dus vergaande beperkingen op te leggen. Echter, zoals dat gaat, juist dan voorziet de wet ook in uitzonderingsmogelijkheden. Zo kan voorbij worden gegaan aan het doelbindingsvereiste als dat nodig is voor, onder andere, de voorkoming, opsporing en vervolging van strafbare feiten, of gewichtige economische en financiële belangen van de staat en andere openbare lichamen, of het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van deze gewichtige economische en financiële belangen (art. 43, onder b t/m d, Wbp, art. 23, eerste lid, onder d, e, g en h, AVG). Ook de bescherming van de belangen van de betrokkenen of anderen kan een reden zijn om voorbij te gaan aan het doelbindingsvereiste (art. 43, onder e, Wbp, art. 23, eerste lid, onder i, AVG).
Voor het optuigen van arrangementen gericht op de aanpak van zorgfraude zal het probleem, of de uitdaging, zijn dat er verzameldoelen worden vastgesteld die voldoende welbepaald zijn, en tegelijkertijd ook de mogelijkheid van data-analyse niet uitsluiten. De verzameldoelen moeten een kader bieden waaraan getoetst kan worden of de gegevens nodig zijn voor die doeleinden of niet. En als we moeten vaststellen dat de verzameldoelen wat dat betreft geen onderscheidend vermogen hebben en eigenlijk alles toelaten, betekent het dat die onvoldoende welbepaald zijn.[76]
Om deze reden volstaat het waarschijnlijk niet dat zorgaanbieders of -verzekeraars in hun privacyverklaringen opnemen dat de gegevens van hun cliënten kunnen worden gebruikt voor 'analysedoeleinden' of 'de aanpak van fraude'. In plaats daarvan zullen de doeleinden nader moeten worden gespecificeerd, bijvoorbeeld door uiteen te zetten wat voor soort fraude het betreft en welke organisaties daarbij nog meer over de gegevens kunnen beschikken, enzovoort. Waar het gaat om gegevens die in een heel andere context worden verzameld, zoals de

76 *Kamerstukken II* 1997/98, 25982, nr. 3, p. 79.

in de vorige paragraaf genoemde onderwijsresultaten (Cito-toets), zal het gebruik ervan niet snel te verenigen zijn met het doelbindingsvereiste. Er zal dan dus gebruik moeten worden gemaakt van een van de uitzonderingen waarin de wet voorziet. Onze indruk is dat die, waar het gaat om de aanpak van zorgfraude, daarvoor wel de nodige ruimte bieden.

4.4 Profilering

Voor bigdata-analyses zijn verder ook de regels voor profilering van belang. We vinden deze regels met zoveel woorden vooral in de AVG, die wat dit betreft evenwel voortbouwt op regels die in de Wbp werden gesteld voor zogeheten geautomatiseerde besluitvorming (art. 42 Wbp). Het begrip 'profilering' is ruim en omvat elke vorm van geautomatiseerde gegevensverwerking waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd. Het gaat daarbij met name om het analyseren of voorspellen van de beroepsprestaties van de betrokkene, diens economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen (art. 4, onder 4, AVG).
Een betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem of haar anderszins in aanmerkelijke mate treft (art. 42, eerste lid, Wbp, art. 22, eerste lid AVG). In drie gevallen zijn er uitzonderingen mogelijk.

– Een betrokkene heeft dit recht niet (meer) als de profilering nodig is voor de uitvoering van een overeenkomst met de betrokkene: we kunnen daarbij denken aan de situatie waarin een aanbieder van streaming video-on-demanddiensten op basis van profilering, en met gebruikmaking van bigdata-analyses, aan haar abonnees bepaalde programma's of series aanbeveelt (art. 22, tweede lid, onder a, AVG).
– En ook niet als er een wettelijke regeling is die de profilering mogelijk maakt en die voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene (art. 22, tweede lid, onder b, AVG). Een voorbeeld zou hier het SyRI-besluit[77] kunnen zijn dat in het voorgaande al werd genoemd en dat data-analyse ten behoeve van de aanpak van fraude in het sociale domein mogelijk maakt.
– En ten slotte, als restcategorie, ook niet als de gegevensverwerking voor profileringsdoeleinden gebeurt op basis van de uitdrukkelijke toestemming van de betrokkene (art. 22, tweede lid, onder c, AVG).

77 Besluit van 1 september 2014 tot wijziging van het Besluit SUWI in verband met regels voor fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens met inzet van SyRI, *Stb*. 2014, 320; zie daarover Zwenne & Schmidt 2016, p. 310 en 339-341.

Voor de aanpak van zorgfraude is verder nog relevant dat in de wetgeving is bepaald dat er bij de gegevensverwerking voor profileringsdoeleinden alleen gebruik mag worden gemaakt van bijzondere gegevens, zoals gezondheidsgegevens, als de betrokkene daarvoor uitdrukkelijke toestemming heeft gegeven of als er passende maatregelen ter bescherming van de gerechtvaardigde belangen van de betrokkene zijn getroffen (art. 22, vierde lid, jo. art. 9 tweede lid, onder a of g, AVG).
Deze regels zijn streng en, zoals we ook al zagen bij de bespreking van de doelbindingsvereisten, de wetgever voorziet dan al snel in uitzonderingen. Interessant is dat dit welbeschouwd eigenlijk alleen in de AVG is gebeurd. In dezelfde bepaling als die voorziet in uitzonderingen op het doelbindingsvereiste is ook voorzien in de mogelijkheid om voorbij te gaan aan de beperkingen die de wet stelt met betrekking tot profilering (art. 23, eerste lid, AVG).[78]
Wat betekent dit voor het gebruik van bigdata-analyses ten behoeve van de aanpak van zorgfraude? Wij denken wel wat, maar uiteindelijk misschien niet heel veel. Immers, er zal zonder twijfel sprake zijn van profilering in de zin van de wet als er gegevens worden verwerkt voor het opstellen van risicoprofielen, bedoeld om bijvoorbeeld de controle van zorgdeclaraties te intensiveren waar dat het meest oplevert. En ook al leidt die profilering niet meteen tot besluiten met rechtsgevolgen voor de betrokkenen, dan nog zal er al snel sprake zijn van dat hem of haar anderszins in aanmerkelijke mate treft. Om een dergelijke vorm van profilering dan mogelijk te maken, zal dan gebruik moeten worden gemaakt van een wettelijke regeling die de profilering mogelijk maakt en die voorziet in passende maatregelen ter bescherming van de rechten, vrijheden en gerechtvaardigde belangen van de betrokkene. En daarin moet dan ook uitdrukkelijk worden voorzien in mogelijkheden om gezondheidsgegevens, waarvan zoals gezegd al snel sprake zal zijn, te betrekken in de data-analyse. Echter, doordat de AVG voorziet in bruikbare uitzonderingen, kan het zomaar zijn dat uiteindelijk de wet niet heel veel beperkingen oplegt met betrekking tot de profilering door middel van bigdata-analyses ten behoeve van de aanpak van zorgfraude.

78 In het ontwerp wetsvoorstel voor de UwAVG, dat eind 2016 via www.internetconsultatie.nl beschikbaar werd gesteld, zien we dat de wetgever voornemens is van deze uitzonderingsmogelijkheid gebruik te maken, maar alleen voor de gevallen waarin er sprake is van geautomatiseerde individuele besluitvorming, anders dan op basis van profilering, die noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of ter uitvoering van een taak van algemeen belang. Zie art. 30, eerste lid, UwAVG (ontwerp) en MvT (ontwerp), p. 53.

4.5 Transparantie

De privacy- en gegevensbeschermingswetgeving verlangt verder dat de betrokkenen worden geïnformeerd over de verwerking van de hen betreffende persoonsgegevens. Onder de Wbp moeten betrokkenen worden geïnformeerd over de identiteit van degene die verantwoordelijk is voor de gegevensverwerking (de 'verantwoordelijke') en de doeleinden waarvoor de gegevens worden verwerkt, alsmede 'nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen (art. 33, eerste t/m derde lid, art 34, eerste t/m derde lid, Wbp). In het geval de gegevens bij iemand anders dan de betrokkenen zelf worden verkregen, behoeft er evenwel niet te worden geïnformeerd, als dat onmogelijk blijkt of een onevenredige inspanning kost (art. 34, vierde lid, Wbp). Evenmin behoeft er te worden geïnformeerd als de vastlegging of verstrekking van de gegevens bij of krachtens wet is voorgeschreven. In dat geval moeten betrokkenen desgevraagd wel worden geïnformeerd over dat wettelijk voorschrift (art. 34, vijfde lid, Wbp).
Onder de AVG is de regeling niet heel anders, zij het wel dat betrokkenen wel veel uitgebreider en gedetailleerder moeten worden geïnformeerd. Zo moet ook mededeling worden gedaan van de contactgegevens van degene die verantwoordelijk is voor de verwerking en over klachtmogelijkheden, ontvangers van de gegevens, eventuele doorgiftes van gegevens naar landen buiten de EU, et cetera (art. 13, tweede lid, en 14, tweede lid, AVG).
Voor bigdata-analyses is daarbij in het bijzonder van belang dat zowel de Wbp als straks de AVG ook verlangen dat, in het geval er sprake is van profilering, de betrokkenen ook mededeling wordt gedaan van 'de logica die ten grondslag ligt aan de geautomatiseerde verwerking van de hen betreffende gegevens' (art. 42, vierde lid, Wbp, art. 13, tweede lid, onder f, AVG, art. 14, tweede lid, onder g, AVG). Wat daaronder precies moet worden verstaan is nog niet heel duidelijk. Aan de parlementaire geschiedenis van de Wbp kan het voorbeeld worden ontleend van het geval aan een naam bepaalde gegevens worden toegevoegd die zijn bepaald op basis van 'postcodesegmentatie of van statistisch onderzoek' (zeg 'verhoogd incassorisico'). In zo'n geval kan de betrokkene erop aanspraak maken dat hem wordt medegedeeld welke methoden zijn gebruikt om daartoe te komen. Als het gaat om algemeen toegankelijke kennis geldt dit echter niet. Zo is algemeen bekend dat een levensverzekeraar het overlijdensrisico op kortere termijn van een tachtigjarige hoger inschat dan dat van een veertigjarige. De verzekeraar is niet gehouden daarover nadere uitleg te geven. Dat is anders als het gaat het om minder voor de hand liggende verbanden bijvoorbeeld op grond van eigen ongepubliceerde statistische recherches.[79]

79 *Kamerstukken I* 1999/2000, 25892, nr. 92c, p. 13.

Met een en ander wordt beoogd de betrokkene, over wie in het kader van de aanpak van zorgfraude met bigdata-analyses gegevens worden verwerkt, in staat te stellen kennis te hebben van wat er over hem bekend is en wat daarvan de gevolgen kunnen zijn. Echter, evenals bij het doelbindingsvereiste (zie par. 3.2) voorziet de wet ook hier in betrekkelijk algemeen geformuleerde uitzonderingen (art. 43, onder b t/m e, Wbp, art. 23, eerste lid, onder d, e, g t/m i, AVG). Het is onze indruk dat daarvan al snel gebruik kan worden gemaakt als het gaat om bigdata-analyses en de aanpak van zorgfraude. Als het al niet gaat om de voorkoming, opsporing en vervolging van strafbare feiten dan kan er zomaar sprake zijn van gewichtige economische en financiële belangen van de staat en andere openbare lichamen of het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van deze belangen. Ook zal er al snel sprake kunnen zijn van de bescherming van belangen of rechten en vrijheden van anderen.

5 Afsluiting: is het genoeg allemaal?

De vraag is of de privacy- en gegevensbeschermingswetgeving in voldoende mate in staat is de waarborgen te bieden die nodig zijn om de rechten van betrokkenen goed te beschermen. De beantwoording van deze vraag veronderstelt een raamwerk waarbinnen kan worden bepaald wat genoeg is, en wat niet. De wetgeving biedt enig houvast bij de constructie daarvan. Van de in de vorige paragraaf verkende regels zien we dat die voor het gezondheidsgegevens en profileren (resp. par. 4.1 en 4.3) erop neerkomen, of in elk geval moeilijk te vermijden maken, dat er voor bigdata-analyses ten behoeve van de aanpak van zorgfraude wordt voorzien in een wettelijke regeling. In die regeling moet dan ook zijn voorzien in passende waarborgen voor de bescherming van deze rechten. En passend betekent in dat verband dat in die regeling de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet wordt gelaten en in een democratische samenleving een noodzakelijke en evenredige maatregel (vgl. art 23, eerste lid, AVG). We komen dan vanzelf uit bij het EVRM, IVBPR en HvEU. Enig houvast kan dan worden gevonden in de rechtspraak van het Europees Hof voor de Rechten van de Mens en het Hof van Justitie van de Europese Unie over heimelijke surveillance en grootschalige gegevensverwerking.[80]

80 Zie bijv. recent HvJ EU 21 december 2016, gevoegde zaken C-203/15 en C-698/15 (Tele2 Sverige); HvJ EU 6 oktober 2015, Mediaforum 2015-7, p. 281-285 (Schrems), m.nt. W. Steenbruggen en S. van Harten en EHRM 4 december 2015, *Computerrecht* 2016-86 (Roman Zakharov), m.nt. S.J. Eskens. Zie voorts Zwenne en Steenbruggen 2015 waarin aan de hand van rechtspraak van het HvJ EU en het EHRM een aantal vuistregels wordt geformuleerd voor de inrichting van grote overheidsinformatiesystemen die ook relevant (kunnen) zijn bij de inzet van big data tegen zorgfraude.

Literatuur

Van Berkhout en Van Engers 2012
T. van Berkhout & T. van Engers 'Onderzoeksmethodologie voor informatiegestuurd sociaal toezicht', *WFR* 2012/824.

Custers 2014
B.H. Custers, 'Risicogericht toezicht, profiling en Big Data', *Tijdschrift voor Toezicht* 2014/5.

Van der Ende 2015
T.A.M. van der Ende, 'Zorgfraude: van handhaving en hoe systemen hun eigen ongelukken creëren', in: J.G. Sijmons e.a., *Op weg naar 10 jaar nieuw zorgstelsel: terug- en vooruitblik*, Preadvies VGR 2015, Den Haag: Sdu Uitgevers 2015, p. 174 e.v.

Hildebrandt (2012)
M. Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era', in: J. Bus et al. (Eds.), *Digital Enlightenment Yearbook*, 2012.

Hildebrandt (2016)
M. Hildebrandt, 'Data-gestuurde intelligentie in het strafrecht', in: *Homo Digitalis*, NJV-preadvies 2016: Deventer 2016.

Olsthoorn 2016
P. Olsthoorn, *Big Data voor Fraudebestrijding*, WRR: Den Haag 2016.

WRR 2016
WRR, *Big data in een vrije en veilige samenleving*, Amsterdam: Amsterdam University Press 2016.

Zorgverzekeraars Nederland 2014
Zorgverzekeraars Nederland, Rapportage controle en fraude 2014.

Zorgverzekeraars Nederland 2015
Zorgverzekeraars Nederland, Rapportage controle en fraude 2015.

Zwenne en Steenbruggen 2016
G.J. Zwenne & W. Steenbruggen, 'Privacyvoorwaarden voor de iOverheid. Vuistregels voor wet- en regelgevers met betrekking tot overheidsinformatiesystemen', *Regelmaat* 2015/1, p. 19-36.

Zwenne en Schmidt 2016
G-J. Zwenne & A.H.J. Schmidt, 'Wordt de homo digitalis bestuursrechtelijk beschermd?', in: *Homo Digitalis*, NJV-preadvies 2016; Deventer 2016.

Deel 3
Big data en zorginstellingen

Deel 3A
Big data voor een lerend zorgsysteem

MR. E.B. VAN VEEN

Deel 3B
De juridische uitdagingen voor een zorginstelling bij big data

MR. T.G. KLEEFMAN

Deel 3
Big data en zorginstellingen

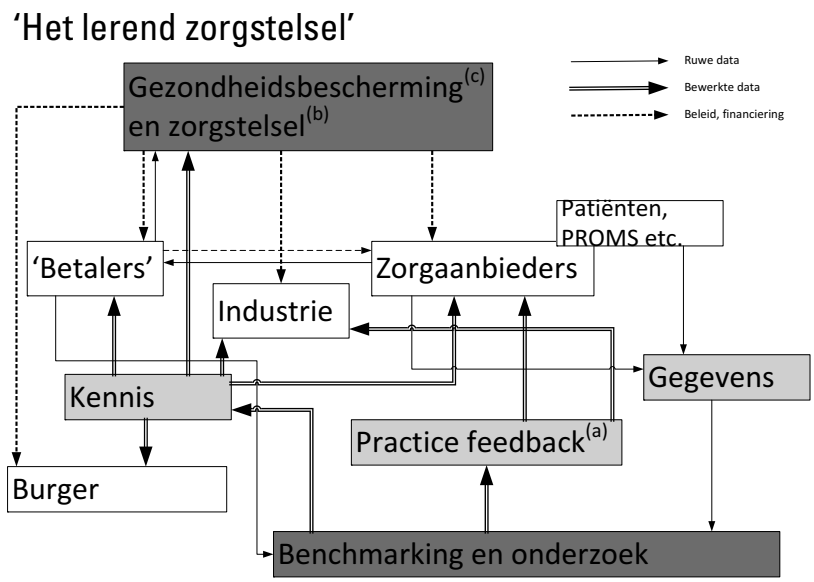
Deel 3A
Big data voor een lerend zorgsysteem

Mr. E.B. van Veen*

* Evert-Ben van Veen is senior adviseur bij en directeur van MedLawconsult en de MLC Foundation te Den Haag.
Met dank aan Michael Klos voor diens hulp bij de referenties. Het schema is een extrapolatie van een schema dat door Dinny de Bakker op een symposium van TRANZO werd gepresenteerd. Alle internetreferenties zijn voor het laatst bezocht op 31-12-2016. In het kader van de transparantie hecht ik eraan op te merken dat ik was betrokken bij de reglementen van een aantal van de in de tekst genoemde kwaliteitsregistraties.

1 Inleiding

Dit hoofdstuk staat in het teken van gegevens voor 'een lerend zorgsysteem'. Dit concept is onder de term 'a learning health care system' ontwikkeld in de Verenigde Staten en heeft aldaar geleid tot een grote hoeveelheid literatuur.[1] In de kern betekent een lerend zorgsysteem dat routinegegevens uit de zorg worden hergebruikt om de zorg te verbeteren. Daarin ligt ook het verschil tussen dit deel van het preadvies en dat van Menno Mostert. Het gaat in dit deel uitsluitend om gegevens die op grond van de professionele standaard al opgetekend (zouden) moeten worden en om gegevens die specifiek ten behoeve van verbetering van de kwaliteit van zorg worden verzameld zoals patiëntervaringen, bijvoorbeeld PROMS[2]. Vervolgens wordt het onderscheid diffuus. Ook standaardgegevens uit de zorg moeten op wetenschappelijk verantwoorde wijze verzameld en verwerkt worden. Dergelijke gegevens kunnen, zoals uit het schema in figuur 1 blijkt, ook leiden tot nieuw wetenschappelijk onderzoek.
Schematisch kan een lerend zorgsysteem worden weergegeven als in figuur 1.



Figuur 1: Lerend zorgsysteem

1 Zie par. 3.1.

2 PROMS staat voor patient reported outcomes measures: 'gevalideerde, eenvoudige vragenlijsten voor patiënten die inzicht geven in de medische effectiviteit van de door een zorgaanbieder geleverde zorg'. Naast PROMS zijn er ook PREMS: een bij voorkeur korte vragenlijst voor de patiënt die vraagt naar de ervaringen met het zorgproces (structuur en proces). Meer hierover zie: https://www.patientervaringsmetingen.nl/wat-is-proms-cq-index/.

Zoals elk schema doet ook dit schema niet geheel recht aan de werkelijkheid. Bijvoorbeeld burgers dragen bij aan observationeel onderzoek via vragenlijsten et cetera. Het gaat hier om de cyclus van gegevens zoals die vanuit de zorg beschikbaar komen en terug worden geleid naar de aanpassing van de praktijk en het beleid. Hoewel meer 'leerdoelen' kunnen worden onderscheiden, zoals de veiligheid van medicijnen en medische hulpmiddelen, concentreer ik mij op de volgende 'leerdoelen' van een lerend zorgsysteem (in het schema aangeduid met een kleine letter):

a. kwaliteitsverbetering door zorgaanbieders[3];
b. informatie ten behoeve van de discussie over de inrichting van het zorgstelsel (en de consequenties van die inrichting);
c. informatie ten behoeve van de discussie over de consequenties van het systeem van gezondheidsbescherming.

Inherent aan een lerend zorgsysteem is dat daarbij het hergebruik van patiëntgegevens essentieel is. Dat roept de vraag op onder welke voorwaarden die gegevens voor een lerend zorgsysteem mogen of misschien zelfs moeten worden hergebruikt. Deze vraag vormt het voornaamste onderdeel van mijn bijdrage.

2 Opbouw

In de volgende paragraaf wordt nader ingegaan op de oorsprong van het begrip lerend zorgsysteem.
Vervolgens wordt ingegaan op voorbeelden van gegevensverwerking in Nederland die als een lerend zorgsysteem kan worden aangemerkt. Bij die bespreking wordt enige kennis van de Wet bescherming persoonsgegevens (Wbp) en de regeling van de geneeskundige behandelingsovereenkomst (WGBO), met name de artikelen 7:457 en 4:458 BW, bekend verondersteld.
Daarna doe ik een stap terug. Mogen wij van zorgaanbieders, overheid en patiënten verwachten bij te dragen aan een lerend zorgsysteem? Die vraag beantwoord ik bevestigend. Dat opent de weg voor een kritische discussie over de huidige voorwaarden voor zulke gegevensverwerking. Daarbij zal ook worden ingegaan op het voorstel voor de Uitvoeringswet van de Algemene Verordening Gegevensbescherming (AVG)[4] zoals dat kort voor het afsluiten van dit hoofdstuk via een internetconsultatie beschikbaar kwam.[5]

---

3 Zorgaanbieders hier in de zin van de Wkkgz.

4 Voluit: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119).

5 https://www.internetconsultatie.nl/uitvoeringswetavg. De conceptuitvoeringswet wordt hierna aangeduid als de UAVG.

De vraag of het bij een lerend zorgsysteem om big data gaat, zoals elders in dit preadvies gedefinieerd,[6] laat ik in het midden. Vastgesteld kan worden dat het in ieder geval gaat om veel gegevens. Met de PROMS et cetera is er ook een zekere 'variety'. Bij leerdoel c zal nog meer variety zijn indien daar ook andere bronnen bij worden betrokken, zoals omgevingsvariabelen. Maar snel gaat die terugkoppeling meestal niet. De gegevens komen vaak pas na een jaar of nog langer beschikbaar.

3 De achtergrond van een lerend zorgsysteem

3.1 Korte blik op de discussie in de VS

De discussie in de VS startte met een workshop van het Institute of Medicine (IOM) en het daarop in 2007 verschenen verslag.[7] Inmiddels heeft het IOM een aparte website over het lerend zorgsysteem.[8] Een lerend zorgsysteem wordt daar inmiddels[9] omschreven als een systeem waarin:

> 'science, informatics, incentives, and culture are aligned for continuous improvement and innovation, with best practices seamlessly embedded in the delivery process and new knowledge captured as an integral by-product of the delivery experience.'[10]

Dit wordt geïllustreerd aan de hand van een van de vele varianten op de 'plan, do, check, act'-cyclus, hier: verzamelen van gegevens (vooral patiëntgegevens), analyseren, interpreteren, terugkoppeling en verandering. Dit schema lijkt sterk op de recente 'kwaliteits- en doelmatigheidscyclus' (K&D-cyclus) in het Nederlandse debat: beschrijven van goede zorg, toepassen en uitvoeren, meten en evalueren.[11]
Zoals ook blijkt uit het verslag van de workshop uit 2007, is een van de doelen van het lerend zorgsysteem volgens het IOM het tijdig kunnen integreren van nieuwe wetenschappelijke kennis in het zorgstelsel. Dat is ruimer dan waar dit hoofdstuk over handelt, namelijk kennis die wij verkrijgen via 'nader gebruik'

---

6 Dit preadvies, hoofdstuk 1a.
7 L. Olsen et al., *The learning healthcare system: Workshop summary (IOM roundtable on evidence-based medicine)*, Washington, DC: National Academies Press 2007.
8 http://www.learninghealthcareproject.org/.
9 Voor zover ik kan overzien zijn de definities in de loop der tijd aangepast.
10 http://www.learninghealthcareproject.org/section/background/learning-healthcare-system.
11 *Kamerstukken II* 2016/17, 29248, 32620, nr. 294.

van patiëntgegevens voor verbetering van de zorg.[12] Wetenschappelijke kennis kan uiteraard ook op andere wijze worden verkregen zoals via laboratoriumexperimenten, wetenschappelijk onderzoek in de zin van de Wet medisch wetenschappelijk onderzoek met mensen en – overigens daarmee soms samenvallend – observationeel onderzoek via cohorten met vrijwilligers, al dan niet met verdere analyse van lichaamsmateriaal.[13] Wetenschappelijk onderzoek met behulp van patiëntgegevens valt er wel binnen en is, zoals de volgende paragraaf laat zien, een belangrijke bron voor evaluatie van de zorgverlening, het zorgstelsel en het systeem van gezondheidsbescherming.

Met name over dat hergebruik van patiëntgegevens handelde een invloedrijk artikel van Faden et al. uit 2013.[14] De achtergrond van dit artikel is mede het strikte regiem in de VS voor wetenschappelijk onderzoek met gegevens in de zorg. Een aantal verbeteringen in de patiëntenzorg waarvoor redelijk bewijs was dat deze beter zouden werken en die volgens het (Nederlandse) principe 'geen implementatie zonder evaluatie' systematisch werden bijgehouden (ook in vergelijking met de zorgaanbieders waar dit niet was doorgevoerd), zou als 'human subjects research'[15] moeten worden aangemerkt, met alle strikte voorwaarden van dien.

Net als bijvoorbeeld Lynn[16] proberen Faden c.s. een onderscheid te maken tussen waar systematische kwaliteitsverbetering ophoudt en 'human subjects research' begint. Belangrijker is het ethische beoordelingskader voor een lerend zorgsysteem in het artikel en daarmee, wat mij betreft, voor zorg in het algemeen. Het is aanzienlijk genuanceerder dan het schema van vier ethische principes uit het befaamde handboek van Beauchamp en Childress over de principes van bioethiek. Dezen onderscheiden vier basisprincipes, namelijk respect voor autono-

12 Op de term 'nader gebruik' kom ik overigens nog terug. Alle patiëntgegevens berusten namelijk op 'nader gebruik'.

13 Waarvan vele voorbeelden, zonder ook maar enigszins volledig te zijn: de inmiddels afgesloten EPIC-studie (de data worden nog steeds geanalyseerd), Lifelines in Groningen, Generation R in Rotterdam, het tweelingenregister van het VUMC.

14 R.R. Faden et al., 'An ethics framework for a learning health care system: a departure from traditional research ethics and clinical ethics', *Hastings Center Report 43/s1* 2013, p. S16–S27.

15 Human subject research in de VS heeft een veel bredere reikwijdte dan onze WMO. Zie voor een beschrijving, in overigens een geheel andere context, J.Grimmelmann, 'The Law and Ethics of Experiment on Social Media Users', *13 Colo. Tech. L.J.* 219, 2015, o.a. downlaodbaar onder https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2604168.

16 Zie ook J. Lynn, 'When does quality improvement count as research? human subject protection and theories of knowledge', *Quality and Safety in Health Care* 13/1 2007, p. 67–70 al veel eerder over dit onderscheid ook W. Lowrance, 'Learning from experience: privacy and the secondary use of data in health research', *Journal of Health Services Research & Policy* 2003/8 suppl 1, p. 2–7.

mie, geen kwaad doen, weldoen en rechtvaardigheid.[17] Faden c.s. onderscheiden in de context van een lerend zorgsysteem zeven principes. De eerste is respect voor de rechten en waardigheid van patiënten, de laatste richt zich – anders dan gebruikelijk is bij de discussies omtrent de inrichting van de zorg – specifiek tot patiënten. Die zouden onder omstandigheden, waarbij uiteraard de weging met andere beginselen een rol speelt, aan een lerend zorgsysteem moeten bijdragen. Ik kom daarop terug.

3.2 Onderdeel van een bredere discussie

Zoals ook uit de volgende paragraaf blijkt, is in Nederland momenteel[18] al in belangrijke mate sprake van een lerend zorgsysteem, zij het niet onder die noemer. Een enkele keer wordt het begrip in Kamerstukken genoemd.[19] Ook in Europese beleidsdocumenten komt men 'learning health care' tegen.[20]
De benaming is op zich niet zo belangrijk. Bijvoorbeeld met de term 'value based health care' lijkt hetzelfde te worden bedoeld.[21] Deze term is ontwikkeld door Michael Porter in een baanbrekend artikel voor de situatie in de VS.[22] Ook daar start het 'met het meten en bespreken van uitkomsten' (van de zorg).[23] Dat loopt parallel met de al genoemde kringloop van gegevens. En zoals de K&D-cyclus laat zien[24] wordt met enige beperkingen, waarop ik in de volgende paragraaf terugkom, in Nederland zo'n kringloop ook nagestreefd.
Over hergebruik van patiëntgegevens verscheen in 2013 ook een OECD-rapport. Aan de hand van een groot aantal voorbeelden benadrukt dit rapport het belang

17 T.L. Beauchamp & J.F. Childress, *Principles of biomedical ethics*, New York: Oxford University Press 2013. Overigens zijn de principes en de rangorde die deze lijken te veronderstellen, in de opvolgende drukken sterk genuanceerd.
18 Met name door de wijzigingen in de Zorgverzekeringswet (Zvw), zoals in par. 4.1 worden behandeld.
19 Senator Bredenoord bij de mondelinge behandeling van de Wkkgz *Handelingen I* 2015/16, 2, nr. 8, p. 17-18.
20 Bijv. in het persbericht: Council conclusions on strengthening the balance in the pharmaceutical systems in the EU and its member states 2016, http://www.consilium.europa.eu/en/press/press-releases/2016/06/17-epsco-conclusions-balance-pharmaceutical-system/ laatst bijgewerkt op 12 december 2016.
21 Zie de blog van Paul van der Nat, 'Value based health care gedijt bij Hollandse cultuur van transparantie', *Skipr*, https://www.skipr.nl/blogs/id2899-value-based-healthcare-gedijt-bij-hollandse-cultuur-van-transparantie.html (d.d. 31 oktober 2016). Mogelijk pas toegankelijk na aanmelden op de Skipr-site.
22 M.E. Porter, 'A Strategy for Health Care Reform — Toward a Value-Based System', *N Engl J Med* 2009; 361:109-112.
23 Van der Nat 2016.
24 *Kamerstukken II* 2016/17, 29248, 32620, nr. 294.

van hergebruik van gezondheidsgegevens om de gezondheid van de bevolking en de veiligheid, effectiviteit en oriëntatie op de patiënt van zorgsystemen te vergroten.[25]
Er is daarmee sprake van een brede beweging.

4 Elementen van een lerend zorgsysteem in Nederland

4.1 Bij leerdoel a

4.1.1 Vooraf

Een lerend zorgsysteem moet worden onderscheiden van de bredere discussie over kwaliteit van zorg,[26] ook al bestaat tussen beide een grote overlap. Uiteraard is het doel van een lerend zorgsysteem om aan de kwaliteit van zorg bij te dragen. Dus kwaliteit van zorg is in die zin het overkoepelende begrip. Tegelijk is een lerend zorgsysteem ook weer breder. Een lerend zorgsysteem geeft ons ook feedback over de inrichting van het zorgstelsel en het systeem van gezondheidsbescherming. Dit zijn leerdoelen b en c die in de regel niet tot de discussie over kwaliteit van zorg gerekend worden. In deze sectie gaat het om leerdoel a.
Ook dan is de gegevensverwerking voor het lerend zorgsysteem niet volledig gelijk aan de meer algemene discussie over kwaliteit van zorg. Het verschil zit in wat er wordt gemeten en op welke wijze dit wordt teruggekoppeld. Bij een lerend zorgsysteem worden gegevens uit de zorg gebruikt voor de berekening van indicatoren die een 'comply or explain'-karakter hebben dan wel als streefwaarden gelden. Bij kwaliteit van zorg kan het ook gaan om indicatoren die een 'alles of niets'-karakter hebben en bij niet-compliance kunnen leiden tot sancties.
Samenhangend met dit verschil in indicatoren is ook de wijze van terugkoppeling van belang. Krijgen zorgaanbieders en individuele hulpverleners deze terug als geaggregeerde gegevens over de eigen performance waarbij op indicatoren wordt vergeleken met het landelijk gemiddelde (benchmarking) om zich via deze spiegelinformatie te verbeteren (of ten minste daarvoor de handvaten te hebben) of wordt top-down teruggekoppeld over wat dan als niet-compliance wordt gezien. Hoewel de betrokken zorgaanbieder daarvan vast ook zal leren, is dat laatste niet het lerend zorgsysteem dat een meer dynamische interactie veronderstelt tussen metingen en aanpassingen, namelijk mogelijk ook van de standaarden.
Daarbij gaat het bij leerdoel a om feedback over de huidige werkwijze en arrangementen aan zorgaanbieders en de daaraan verbonden hulpverleners. Die feed-

25 OECD, *Strengthening health information infrastructure for health care quality governance good practices, new opportunities and data privacy protection challenge: OECD health policy studies*, Paris: Organization for Economic Co-operation and Development (OECD) 2013.

26 Zie m.n. Kamerstukken onder nr. 31765 voor die discussie.

back biedt evenzoveel uitdagingen voor verbetering. Die feedback geschiedt aan de hand van bepaalde uitgangspunten. Gegevens zonder context zijn waardeloos.

4.2.1 De voorbeelden

De voorbeelden hier zijn de vele kwaliteitsregistraties die inmiddels in Nederland bestaan. Ik moge verwijzen naar een aantal websites, zoals www.dica.nl (waaronder een groot aantal afzonderlijke kwaliteitsregistraties) en www.lroi.nl. Met uitzondering van de geestelijke gezondheidszorg (zie www.sbggz.nl), zijn deze kwaliteitsregistraties als het ware van onderop ontstaan voornamelijk vanuit de betrokken wetenschappelijke verenigingen van, zoals dat toen heette, de Orde van Medisch Specialisten.[27] En nog steeds lijken kwaliteitsregistraties voornamelijk een bottom-upactiviteit in die zin dat zij van de beroepsbeoefenaren uitgaan, niet van de zorgaanbieders.[28] Voor zover mij bekend[29] hebben de initiatiefnemers artikel 4 van de toenmalige Kwaliteitswet zorginstellingen (KWZi)[30] zelden als grondslag gebruikt. Zorgaanbieders werden vervolgens aangehaakt vanwege de veranderingen op de zorgmarkt op grond waarvan zorgverzekeraars selectief konden inkopen en waaraan onder andere al dan niet zelfbedachte kwaliteitscriteria ten grondslag lagen.[31] Via de kwaliteitsregistraties konden min of meer objectieve gegevens over de geboden kwaliteit worden aangeboden die de zorgverzekeraars dan niet meer bij de zorgaanbieders afzonderlijk zouden hoeven uit te vragen. In dat opzicht speelden de zorgaanbieders wel een rol, namelijk dat deze met de ontsluiting van 'hun' kwaliteit via de kwaliteitsregistratie moeten instemmen.
Het speelveld rond de kwaliteitsregistraties is aanzienlijk veranderd sinds de wijzigingen van de Zorgverzekeringswet (Zvw), de Wkkgz (nt. 30) en diens voorloper, naast de genoemde KWZi, het veel bediscussieerde wetsontwerp cliëntenrechten zorg.[32] Hoewel laatstgenoemd wetsontwerp onder die noemer nooit het *Staatsblad* heeft gehaald, traden enkele onderdelen, met name de bevoegdheden van het Zorginstituut Nederland (ZIN) met betrekking tot de kwaliteit van zorg al op 1 april 2014 in werking.[33]

---

27 Inmiddels de Federatie Medisch Specialisten.
28 Bijv.: https://www.medischcontact.nl/nieuws/laatste-nieuws/artikel/obstakels-bij-een-registratiesysteem.htm.
29 Ik was toen bij een aantal kwaliteitsregistraties betrokken.
30 Wet van 18 januari 1996. De KWZi is ingetrokken bij de inwerkingtreding van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz), zie verder de tekst.
31 Over deze ontwikkeling ook J.G. Sijmons, 'Inleiding' in: *Preadvies 2015 Vereniging voor Gezondheidsrecht – Op weg naar 10 jaar nieuw zorgstelsel, terug- en vooruitblik*, Den Haag: Sdu, p. 13-30.
32 *Kamerstukken* 33243.
33 *Stb.* 2014, 93.

4.2 De huidige juridische grondslagen voor deze gegevensverwerking

Onderscheiden moeten worden:
a. de bepalingen die tot kwaliteitsregistraties leiden; en
b. de voorwaarden waarbinnen deze 'privacy compliant' (de Wbp en WGBO in onderlinge samenhang) mogen worden uitgevoerd.

Ad a
In essentie zijn thans twee artikelen relevant als grondslag voor deze gegevensverwerking. Het eerste is artikel 7 Wkkgz, het tweede artikel 66d Zvw. Artikel 7 Wkkgz luidt voor zover hier relevant en met mijn cursivering als volgt:

> 'a. De zorgaanbieder draagt zorg voor systematische bewaking, beheersing en verbetering van de kwaliteit van de zorg. De verplichting van het eerste lid houdt, de aard en omvang van de zorgverlening in aanmerking genomen, in:
> b. het op systematische wijze verzamelen en registreren van gegevens betreffende de kwaliteit van de zorg *op zodanige wijze dat de gegevens voor eenieder vergelijkbaar zijn met gegevens van andere zorgaanbieders van dezelfde categorie*;'

Artikel 7 is sterk vergelijkbaar met het al genoemde artikel 4 van de KWZi maar de gecursiveerde zinsnede is nieuw. De vraag is uiteraard hoe zorgaanbieders vergelijkbaar kunnen registreren indien zij niet weten wat andere vergelijkbare zorgaanbieders registreren. Met andere woorden, de gecursiveerde zinsnede veronderstelt een zekere centrale regie.
Hier spelen de door de kwaliteitsregistraties opgestelde indicatoren een rol. Om deze indicatoren is veel te doen geweest.[34] Los van de discussie waarom en waartoe wordt gemeten, leek er soms ook sprake van een zeker 'hobbyisme' waar de koplopers in de beroepsgroep een veelheid van indicatoren vaststelden die de ziekenhuizen vervolgens moesten registreren.[35] Het veld heeft het initiatief genomen om orde te brengen in de veelheid van initiatieven.[36]
De tweede grondslag is via de bepalingen van de Zvw en de 'doorzettingsmacht' van het ZIN. Het gaat met name om de volgende bepaling (artikel 66d Zvw):

---

34 Met name in *Medisch Contact*, zie een positieve visie bij bijv.: https://www.medischcontact.nl/nieuws/laatste-nieuws/artikel/Kwaliteitsregistraties-maken-de-zorg-beter.htm en voor een negatieve visie https://www.medischcontact.nl/nieuws/laatste-nieuws/artikel/kwaliteitsindicatoren-maken-zorg-slechter.htm. Zie *Kamerstukken II*, 2011/12 32620, nr. 29.
35 https://www.medischcontact.nl/nieuws/laatste-nieuws/artikel/registreren-terugkoppelen-en-publiceren.htm.
36 https://www.landelijkekwaliteitsregistratie.nl/.

'1 Het Zorginstituut draagt zorg voor het verzamelen, samenvoegen en beschikbaar maken van informatie over de kwaliteit van verleende zorg:
a. met het oog op het recht van de cliënt een weloverwogen keuze te kunnen maken tussen verschillende zorgaanbieders, en
b. ten behoeve van het toezicht door de ambtenaren van het Staatstoezicht op de volksgezondheid.
2 Zorgaanbieders zijn verplicht de informatie, bedoeld in het eerste lid, te rapporteren op basis van de overeenkomstig artikel 66 b in het openbaar register opgenomen meetinstrumenten.'

De ordening komt met name vanuit het toetsingskader kwaliteitsstandaarden van het ZIN en het daaraan verbonden Kwaliteitsinstituut.[37] In de meest recente versie[38] worden drie elkaar opvolgende elementen onderscheiden, namelijk:
– de kwaliteitsstandaard;
– de informatiestandaard;
– het meetinstrument.
Deze drie kunnen niet zonder elkaar. Meetinstrumenten kunnen niet los worden gezien van informatiestandaarden, die op hun beurt afhankelijk zijn van een kwaliteitsstandaard. Voor de informatiestandaarden wordt aangesloten bij 'eenmalige invoer, meervoudig gebruik'.[39] Met andere woorden, geen indicatoren die niet ook in het kader van de patiëntenzorg op grond van artikel 7:454 BW moeten worden opgetekend.[40] Het is dan overigens een andere vraag of EPD-systemen van ziekenhuizen het mogelijk maken dat deze gegevens met een druk op de knop naar de desbetreffende kwaliteitsregistratie worden uitgevoerd of dat deze nog steeds vanuit de zorgaanbieder handmatig moeten worden ingevoerd.
Het ZIN heeft voor de aanlevering van de artikel 66d-gegevens 'informatiemakelaars' aangewezen. Een regeling aanwijzing gegevensmakelaars heb ik niet kunnen vinden en evenmin de specifieke aanwijzing welke gegevensmakelaars voor welk type behandelingen of zorgaanbieders zijn aangewezen. Het blijkt indirect.[41] Daarbij blijkt ook dat de landelijke kwaliteitsregistraties deze gegevensmakelaars zijn en een intermediaire rol vervullen tussen artikel 7 Wkkgz en artikel 66d Zvw.

37 Zie https://www.zorginstituutnederland.nl/kwaliteit/het+kwaliteitsinstituut.
38 Zorginstituut Nederland, Toetsingskader kwaliteitsstandaarden informatiestandaarden & meetinstrumenten 2015, op: https://www.zorginstituutnederland.nl/.
39 NFU, Registratie aan de bron. Visie op documentatie en gebruik van zorggegevens 2013-2020, 2013 Zoek op: https://www.nfu.nl.
40 Bij m.n. de indicatoren voor de DICA-registraties was dat naar mijn ervaring wel anders.
41 Zoals bij: https://www.zorginstituutnederland.nl/kwaliteit/aanleveren+kwaliteitsgegevens/transparantiekalender.

Zorgaanbieders leveren niet afzonderlijk aan maar via het aggregaat zoals dat bij de kwaliteitsregistratie beschikbaar is. Vanuit de kwaliteitsregistratie naar ZIN gaat trouwens niet zonder de nodige ICT die dit mogelijk maakt. Dutch Hospital Data (DHD, ik kom daar nog op terug) heeft daarvoor het OmniQ-platform ontwikkeld.[42]
Oorspronkelijk leek de minister de uitkomsten op de indicatoren haast uitsluitend te zien in het kader van de transparantie en informatie voor patiënten welke zorgaanbieder te kiezen.[43] Hoe nuttig dit soort informatie[44] ook moge zijn, er zijn ook aanwijzingen dat de gemiddelde patiënt niet zo kiest.[45] Mede daarom is wat mij betreft het daaraan voorafgaande proces veel belangrijker. Dat is de terugkoppeling aan de zorgaanbieders over de eigen performance vergeleken met de benchmark vanuit de kwaliteitsregistraties waaruit het transparantieportaal wordt gevoed. Overigens worden de uitkomsten nu breder toegepast, namelijk ook om 'samen beslissen' te ondersteunen en in dat kader hulpmiddelen te ontwikkelen. Dat wil zeggen voor welke opties bij een bepaalde aandoening, als al voor een hulpverlener 'gekozen' is.[46] Dat zou inderdaad een ander mooi voorbeeld van 'nader gebruik' in het kader van de meten-en-evaluerencyclus zijn.

Ad b
Tussen registreren bij de zorgaanbieder en aanbieden aan het ZIN zitten voornoemde kwaliteitsregistraties. In die tussenliggende fase is sprake van bijzondere persoonsgegevens. Zij zijn nogal genuanceerd, ook om zogenaamde casemixcorrectie[47] toe te kunnen passen, en zorgaanbiederoverstijgend. Een belangrijke indicator bij veel standaarden is bijvoorbeeld heropname binnen zoveel maanden na een operatie (en de reden van de heropname). Die heropname hoeft lang niet altijd bij dezelfde zorgaanbieder plaats te vinden waar de eerste operatie plaatsvond. Vanuit de kwaliteitsregistraties gaat veel sturing uit (met name de informatiestandaarden/indicatoren en meetinstrumenten). In die zin zouden de kwaliteitsregistraties verantwoordelijke zijn in de zin van artikel 1 onder d Wbp, omdat zij immers het doel en de middelen van de gegevensverwerking bepalen. Zij hebben echter geen grondslag om persoonsgegevens te verwerken. Voor de zorgaanbieder zijn zij een derde in de zin van artikel 7:457 BW en voorts vallen zij even-

42 https://www.dhd.nl/klanten/over-ons/nieuws/Paginas/OmniQ---een-portaal-voor-aanlevering-kwaliteitsindicatoren-t.b.v.-Transparantiekalender.aspx.
43 Zie ook *Kamerstuk* 33620 nr. 168. 2016 werd in dat kader tot het jaar van de transparantie uitgeroepen.
44 Zoals deze blijken op www.zorgkaartnederland.nl.
45 M. Levi, W. Bos, 'Weinig keuzebereidheid bij patiënten', *NTvG* 2015:159 (3).
46 *Kamerstukken II* 2016/17, 29248, 32620, nr. 294.
47 Dat betekent dat rekening wordt gehouden met comorbiditeit en andere omstandigheden die de uitkomsten van een verrichting kunnen beïnvloeden zoals BMI en al of niet roken.

min onder artikel 21 Wbp. Toestemming werkt om de in paragraaf 5 te behandelen redenen niet. In de praktijk wordt voor veel registraties de oplossing gezocht door voor alle zorgaanbieders die aan een bepaalde kwaliteitsregistratie deelnemen één bewerker in de zin van artikel 1 onder e Wbp tussen te schakelen tussen hen en de organisator van de kwaliteitsregistratie. De verantwoordelijke zorgaanbieder geeft dan opdracht om de gegevens te bewerken aan de hand van de indicatoren en naar de organisator van de kwaliteitsregistratie uit te voeren.
Het systeem wringt. Zogenaamd blijven de zorgaanbieders verantwoordelijken, tegelijk moeten zij wel deelnemen. Voorts zal de kwaliteitsregistratie meer willen met de aldus systematisch verzamelde gegevens, namelijk kunnen ontsluiten voor wetenschappelijk onderzoek. Gelet op de hoge drempel om van anonieme gegevens te kunnen spreken (zie sectie 6.3 infra) zullen dat voor een genuanceerd onderzoek niet altijd anonieme gegevens kunnen zijn.[48]
Naar een duidelijker grondslag moet wordt gezocht en die lijkt ook bereikbaar. In paragraaf 7 zal daar nader op worden ingegaan.

4.3 Elementen van een lerend zorgsysteem bij leerdoel b

4.3.1 Vooraf

Hier gaat het om gegevens die in de publieke discussie kunnen worden gebruikt voor beoordeling van het stelsel van gezondheidszorg. In algemene zin is iedereen in Nederland het wel over de uitgangspunten eens, namelijk een stelsel dat optimale kwaliteit biedt, gelijke toegang en houdbaar is op de lange duur.[49] Die elementen zijn niet zonder meer makkelijk verenigbaar. Het wordt nog complexer indien keuzemogelijkheden voor verzekerden worden toegevoegd als een element van de uitganspunten voor het stelsel, zonder daarbij te benoemen of dit is bedoeld om de voornoemde uitgangspunten dichterbij te brengen dan wel dat dit als een zelfstandige waarde voor zo'n stelsel moet gelden. De al genoemde spanning tussen solidariteit en vrijheid. In een mogelijk wat optimistisch scenario is het uitgangspunt hier dat die discussie mede wordt gevoerd op basis van gegevens.

4.3.2 Voorbeelden

Het zorgstelsel valt lastig te sturen maar helemaal niet zonder cijfers, al komen die vaak wat laat. Bij het Centraal Bureau voor de Statistiek (CBS) komen alle cijfers samen.[50] Veel van die cijfers komen overigens van het hierna te bespreken DBC-informatiesysteem (DIS).

---

48 In de reglementen van de mij bekende kwaliteitsregistraties oordeelt daar dan een privacycommissie of vergelijkbaar orgaan over.
49 Bijv. *Kamerstukken II* 2011/12, 29689, nr. 140.
50 https://www.cbs.nl/nl-nl/nieuws/2016/20/zorguitgaven-stijgen-langzamer.

Veel rapporten over mogelijke aanpassingen van het stelsel zijn deels gebaseerd op bestaande cijfers over de werking van het huidige systeem, gevoegd met voorbeelden van elders en min of meer wetenschappelijk gefundeerde veronderstellingen[51] hoe mensen zullen reageren op beleidskeuzes. Het rapport van het Centraal Planbureau (CPB) over 'Zorgkeuzes in kaart' is een voorbeeld van die multidisciplinaire benadering.[52]
Een interessant voorbeeld waar uitsluitend gegevens over de huidige werking van het stelsel werden gebruikt is een ander rapport van het CPB over keuzegedrag van verzekerden en risicosolidariteit bij vrijwillig eigen risico.[53]
Het was een behoorlijk complexe studie waarbij de gegevens van 14 miljoen Nederlanders waren betrokken. Via Zorg TTP werd een koppeling gemaakt tussen gegevens die bij het ZIN op grond van de risicovereveningsdata zijn bekend en bij Vektis, de – al blijkt dat niet direct uit hun website[54] – bewerker in de zin van de Wbp van de zorgverzekeraars in Nederland. Die gegevens betroffen leeftijd, geslacht, zorgkosten, diagnosekostengroep (DKG), farmaciekostengroep (FKG) en de viercijferige postcode. Dit gecombineerde bestand werd vervolgens verrijkt met CBS-gegevens over huishoudensinkomen en het opleidingsniveau gebaseerd op de vier cijfers van de postcode van de 'betrokkenen'.[55]

4.3.3 De juridische grondslagen

Er zijn veel grondslagen waarop de gegevens worden uitgewisseld waardoor het Nederlandse zorgverzekeringsstelsel met die aparte mix van solidariteit[56] en een zekere marktgerichtheid kan functioneren. Patiëntgegevens liggen daaraan ten grondslag[57] naast de aan de zorgverzekeraar bij het aangaan van de zorgverzeke-

51 Zoals via focusgroepen of vragen in panels.
52 https://www.cpb.nl/sites/default/files/publicaties/download/cpb-boek-15-zorgkeuzes-kaart-technische-uitwerking-van-alle-afzonderlijke-beleidsopties.pdf.
53 https://www.cpb.nl/sites/default/files/omnidownload/CPB-Notitie-1nov2016-Keuzegedrag-verzekerden-en-risicosolidariteit-bij-vrijwillig-eigen-risico.pdf.
54 www.vektis.nl.
55 Hier tussen aanhalingstekens. Betrokkene is in Wbp-termen degene op wie een persoonsgegeven betrekking heeft. Het is de vraag of hier van zulke betrokkenen sprake is. Daar wordt in de tekst op teruggekomen.
56 Die solidariteit blijkt niet alleen uit de acceptatieplicht en geringe bandbreedte voor een vrijwillig eigen risico maar ook de daar achterliggende risicoverzekering tussen zorgverzekeraars. Het ZIN berekent deze op basis van jaarlijks door de minister opgegeven waarden (de regeling risicoverevening) en ontvangt daartoe van de zorgverzekeraars vrij gedetailleerde gegevens. Zie art. 35 Zvw ju. 86 en 88 Zvw. Zie ook Tekst en Commentaar Gezondheidsrecht, p. 592-593.
57 J.M.E. Citteur & J.J. Rijken, 'Verstrekken van patiëntengegevens door zorgaanbieders aan zorgverzekeraars', *TvGR* 2013/37 afl. 8, p. 750-763.

ring opgegeven gegevens. Vanwege de acceptatieplicht is die laatste categorie echter gering. Deze gegevensuitwisseling betreft het primaire proces maar dan in financiële zin en behoeft hier niet te worden behandeld. Zoals blijkt uit het laatste voorbeeld uit de vorige sectie kunnen die gegevens vervolgens wel voor een lerend zorgsysteem worden ingezet.
De gegevensverwerking uit het eerste voorbeeld is gebaseerd op de Wet op het CBS. Het CBS mag uit diverse bronnen persoonsgegevens onder het BSN opvragen en verwerken, evenwel uitsluitend ten behoeve van statistische overzichten[58] naast doorlevering aan in de CBS-wet genoemde afnemers. Onder omstandigheden kunnen onderzoekers van de CBS-gegevens gebruikmaken.[59]
Specifiek voor een lerend zorgsysteem bij dit leerdoel is de gegevensverwerking ten behoeve van het DBC-informatiesysteem (DIS).[60] Het DIS is niet bedoeld om zorgaanbieders te financieren maar om over gegevens te beschikken waarmee ontwikkelingen op de zorgmarkt kunnen worden gemonitord. Vanuit de zorgaanbieder gaan 'gepseudonimiseerde' DBC-gegevens over elke patiënt naar het DIS. Vanuit het DIS gingen deze gegevens naar de volgende afnemers: de Nederlandse Zorgautoriteit zelf (NZa, die ook het DIS beheert), CBS, het ZIN en VWS. Over het DIS is veel te doen geweest. Nadat de minister lange tijd had volgehouden dat in het DIS geen persoonsgegevens zouden worden verwerkt,[61] oordeelde de Autoriteit Persoonsgegevens (AP)[62] in april 2016 anders.[63] Overigens oordeelde de AP eveneens dat zorgaanbieders een grondslag hebben om die persoonsgegevens aan de NZa te verstrekken en de NZa om deze te verwerken en aan het CBS en het ZIN door te leveren, evenals aan de Autoriteit Consument en Markt. Niet aan VWS, waarmee die gegevenslevering stopte.[64] Ik kom op de DIS-casus terug bij de beschouwingen in paragraaf 6.
Overigens zijn er geen specifieke grondslagen om gegevens voor dit leerdoel te verwerken en zullen studies, zoals de genoemde CBP-studie over risicosolidariteit en keuzegedrag, met inachtneming van de Wbp, en voor zover relevant de

58 Zoals voor de gezondheidszorg: https://www.cbs.nl/nl-nl/nieuws/2016/20/zorguitgaven-stijgen-langzamer.
59 Art. 41 t/m 42a Wet op het CBS.
60 Zie https://www.dbcinformatiesysteem.nl/over/vertrouwelijkheid-data. Deze site is niet aangepast aan de in de tekst beschreven ontwikkelingen.
61 *Aanhangsel Handelingen II* 2011/12, 2447.
62 Ik gebruik hier de benaming voor het College bescherming persoonsgegevens zoals die sinds 2016 geldt 'in het maatschappelijk verkeer' (art. 51 lid 4 Wbp). Voor de uitspraken van het CBP van voor 2016 gebruik ik de aanduiding zoals die toen gold en die overigens nog steeds de formeel juiste is.
63 AP Z2015-00355 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_nza-dis.pdf.
64 Overigens zou naar mijn mening niet uitsluitend moeten meespelen of de NZa die gegevens mag verstrekken maar of de ontvanger dan zulke bijzondere persoonsgegevens zou mogen verwerken. Dat zou voor VWS eveneens niet het geval zijn.

WGBO, moeten plaatsvinden. Bij de genoemde studie werd dan gebruikgemaakt van 'gepseudonimiseerd-anonieme' gegevens in het doelbestand waarop het CBP de analyses uitvoerde. Ook daarop kom ik in paragraaf 6 terug.

4.4 Elementen van een lerend zorgsysteem bij leerdoel c

4.4.1 Vooraf

Hier gaat het om de effecten van risico's die wij bewust of onbewust lopen en die blijken in de patiëntenzorg. Soms is zorg noodzakelijk door onze inherente kwetsbaarheid, soms komen de oorzaken voor de aandoening van buitenaf in de zin van waar wij eraan blootgesteld worden door te werken of te recreëren. Ook hier zijn uiteraard weer grijze gebieden. Er zijn oorzaken van buiten die men zou kunnen vermijden (al zou men dan eerst moeten weten welke en dat is weer op basis van cijfers). Dezelfde blootstelling heeft lang niet altijd voor elke betrokkene dezelfde consequenties voor zijn gezondheid. Ik moge hopen dat men dan kiest voor de meest kwetsbaren. Zonder te willen treden in de complexe discussie over de grenzen van publieke gezondheidszorg,[65,66] indien gegevens uit de patiëntenzorg niet worden geanalyseerd op mogelijke oorzaken van buitenaf,[67] kan de discussie hoe die oorzaken af te wenden in het geheel niet worden gevoerd.

4.4.2 Voorbeelden

Mooie voorbeelden staan op de site 'de staat van de volksgezondheid en zorg'[68] een initiatief van verschillende partijen dat sinds het najaar van 2016 alle cijfers omtrent de incidentie of prevalentie van aandoeningen of gezondheidsproblemen systematisch ontsluit. Die site toont een rijkdom aan data en de achterliggende bronnen. Overigens komen lang niet alle daar genoemde gegevens via hergebruik van patiëntgegevens beschikbaar maar een belangrijk deel wel, zoals met betrekking tot gegevens over incidentie en prevalentie en overlevingsduur van kanker van het Integraal Kankercentrum Nederland (IKNL). De Nederlandse Kankerregistratie (NKR)[69] speelt een grote rol in het lerend zorgsysteem.

---

65 J. Dute, 'De Wet publieke gezondheid', *TvGR*, 2008/32, afl. 8, p. 576-591.

66 Naast Dute (2008) treffend beschreven, zowel met betrekking tot de terminologie als de inhoud, waar 'public health' in een liberale maatschappij dan uit zou moeten bestaan. J. Coggon, *What makes health public? A critical evaluation of moral, legal, and political claims in public health*, New York: Cambridge University Press 2012, overigens ook: Nuffield Council On Bioethics, *Public health: Ethical issues*, London: Nuffield Council on Bioethics 2007.

67 Hier fungeren patiëntgegevens nog het meest als de kanaries in de kolenmijnen van weleer.

68 https://www.staatvenz.nl/.

69 http://www.cijfersoverkanker.nl/.

Een voorbeeld dat wij toch niet alles tijdig in beeld hebben, is de late detectie van de Q-koortsuitbraak in Brabant, namelijk in 2007. Q-koorts is een zoönose (van dier naar mens overgedragen) en een aangifteplichtige ziekte op grond van artikel 19 Wet publieke gezondheid jo. artikel 12 van het Besluit publieke gezondheid. Dan moet de hulpverlener wel eerst aan Q-koorts hebben gedacht als de mogelijke oorzaak van een asymptomatische longontsteking of hepatitis. Toen Q-koorts nog uiterst zeldzaam was of leek, was dat niet de waarschijnlijkheidsdiagnose. Los van de vraag of de betrokken autoriteiten adequaat hebben gereageerd nadat Q-koorts wel was ontdekt als de oorzaak van een gezondheidsprobleem van de omwonenden van en recreanten rond de geitenstallen,[70] het had ook anders kunnen lopen indien een verheffing van serieuze longklachten bij een op grond van geografische gegevens benoemd cluster van patiënten eerder was ontdekt en daarmee eerder vragen konden worden gesteld over de oorzaak. Een mooie studie met behulp van DHD-gegevens laat zien dat die verheffingen achteraf inderdaad konden worden gedetecteerd. Uit de samenvatting van de studie:

> 'Real-time syndromic surveillance would have detected four of the other [dan de cluster die de bal aan het rollen bracht, E-BvV] clusters in 2007, one in 2006 and two in 2005, which might have resulted in detection of Q-fever outbreaks up to 2 years earlier'.[71]

4.5 Juridische grondslagen

Buiten de Wet publieke gezondheid zijn er geen specifieke grondslagen. De gegevensverwerking ten behoeve van dit doel zal binnen de grenzen van de privacywetgeving moeten plaatsvinden.
De door IKNL onderhouden NKR is gebaseerd op artikel 7:458 BW en daarmee een geen-bezwaarsysteem.
DHD is de bewerker voor alle Nederlandse ziekenhuizen met betrekking tot een door de veldpartijen vastgestelde dataset. Op dat aggregaat van alle ziekenhuizen kunnen analyses worden gedaan. Het aggregaat bevat nog steeds persoonsgegevens. Onderzoekers krijgen dan geen rechtstreekse toegang tot die gegevens maar een anonieme uitvoer op basis van hun zoekvragen. Zo construeer ik het retrospectieve Q-koortsonderzoek.

---

70 Daarover o.a. Evaluatiecommissie Q-koorts, *Van verwerping tot verheffing Q-koortsbeleid in Nederland 2005-2010*, Den Haag 2010. In januari 2017 zal de Rb. Den Haag uitspraak doen in de claim die een groot aantal Q-koortsslachtoffers tegen de Staat heeft aangespannen, zie http://www.qkoortsclaim.nl en http://stichtingquestion.nl voor naar wat lijkt de meest representatieve patiëntenorganisatie.

71 C.C. Van den Wijngaard et al., 'In search of hidden q-fever outbreaks: linking syndromic hospital clusters to infected goat farms', *Epidemiology and Infection* 2011/139 afl. 01, p. 19–26.

5 Intermezzo: wat mag voor een lerend zorgsysteem worden verwacht?

5.1 Twee confronterende uitgangspunten

Dit is de schakelparagraaf tussen hetgeen voorafging en hetgeen volgt. De kop van deze paragraaf noemt niet van wie dat mag worden verwacht. Ik begin met patiënten of burgers in het algemeen. Vandaar volgt de rest.
Voor de patiënten en burgers in het algemeen poneer ik de volgende nogal confronterende uitgangspunten.

1. Men kan niet, met goed fatsoen althans, van twee walletjes eten. Dat wil zeggen: en spreken van jouw (= de patiënt) gegevens met een soort van micromanagement waartoe die gegevens mogen worden ingezet én verwachten te zijn ingebed in een kwalitatief zo goed mogelijk, houdbaar, solidair zorgstelsel en optimaal systeem van gezondheidsbescherming.
2. Er bestaat niet zoiets als unieke, uitsluitend op mij betrekking hebbende patiëntgegevens in de zin van 7:454 BW. Al die gegevens die de hulpverlener moet optekenen, berusten op hergebruik van eerdere patiëntgegevens.

Meer over het eerste uitgangspunt. Deze heeft een morele claim en een empirische. Aan de morele komt men pas als de empirische is behandeld. Die empirische claim is dat het 'van twee walletjes eten' of, aardiger gezegd, 'het beste van twee werelden' niet kan worden bereikt door de 'consent or anonymise'-benadering.[72] Daarover de volgende sectie.

5.2 Consent or anonymise werkt niet om het beste van twee werelden te bereiken

Hoewel, zoals ik in de volgende paragraaf zal betogen, meer gegevens als anoniem kunnen worden aangemerkt dan de AP in diens uitspraak over het DIS heeft gesteld,[73] is een lerend zorgsysteem onmogelijk zonder in de eerdere fases van de analyses – tussen van zorgaanbieder en uitkomsten zitten namelijk vele stappen – niet-anonieme gegevens te verwerken. Hetgeen niet betekent dat tussentijds niet, zoals ik dat met anderen heb genoemd, 'privacyfilters' moeten worden ingezet.[74] Maar ook met die filters, zoals bij voornoemde CBP-studie gebeurde,

---

72 N. Sethi & G. Laurie, 'Delivering proportionate governance in the era of eHealth: Making linkage and privacy work together', *Medical Law International* 2013, Vol 13(2-3) p. 168–204.

73 AP Z2015-00355 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_nza-dis.pdf.

74 W. Kuchinke et al., 'A standardised graphic method for describing data privacy frameworks in primary care research using a flexible zone model', *International Journal of Medical Informatics* 2014/83 afl. 12, p. 941–957.

kan bijvoorbeeld bij die studie de vraag worden gesteld of het doelbestand in de voornoemde studie, wel echt anoniem was. Niet vanwege de pseudonimisering maar vanwege de rijkdom van de daarin opgenomen gegevens die noodzakelijk is voor de analyses (zie ook sectie 6.3 infra). In de publicatie van de toenmalige RVZ getiteld 'Patiënteninformatie'[75] wordt zowel aan die tussenliggende stappen als aan de vraag naar anonimiteit van gegevens te gemakkelijk voorbijgegaan. Privacy en anonimiteit worden daar gelijkgesteld, een andere verkeerde tegenstelling waar ik nog op terugkom.
Dan het alternatief voor volledige anonimisering aan de bron: uitdrukkelijke toestemming die dan om als werkelijk uitdrukkelijk te kunnen worden aangemerkt, ook behoorlijk genuanceerd moet zijn. Los van de kosten van zo'n systeem en de 'consent fatigue', zoals elders beschreven;[76] er bestaat ook zoiets als 'bias'. De in de analyses verwerkte gegevens moeten representatief zijn voor de onderscheiden subgroepen van patiënten. Er bestaan statistische technieken om bias door onder- of overrepresentatie in steekproeven te compenseren maar indien men niet weet wie wel en niet meedoen in de zin van gegevens delen, werken die technieken niet.[77] Naast patiëntenbias zou er bij de kwaliteitsregistraties overigens ook nog eens 'doktersbias' bijkomen. Een hulpverlener die niet wil dat diens kwaliteit wordt getoetst, stelt dat de patiënt geen toestemming heeft gegeven. Voor het overige moge ik verwijzen naar behoorlijk wat literatuur over hoe informed consent voor 'registry research' niet werkt[78] en volledige anonimisering tot onjuiste uitkomsten leidt.[79]

5.3 Alle patiëntgegevens berusten op hergebruik

Nu meer over het tweede uitgangspunt. Uiteraard is elke patiënt uniek in die zin dat wij allemaal hopen dat ons persoonlijke verhaal wordt gehoord.[80] Maar de

75 Raad voor de Volksgezondheid en Zorg, Patiënteninformatie.

76 E.M.L. Moerel, *Big data protection: How to make the draft EU regulation on data protection future proof*, Tilburg: Tilburg University 2014. E.M.L. Moerel & J.E.J. Prins 'Privacy voor de homo digitalis', in: Nederlandse Juristen-Vereniging, *Homo Digitalis*, Amsterdam: Wolters-Kluwer 2016, p. 1–136.

77 S. Rebers et al., 'A randomised controlled trial of consent procedures for the use of residual tissues for medical research: preferences of and implications for patients, research and clinical practice', *PLOS ONE* 2016/11 afl. 3.

78 J.R. Ingelfinger & J.M. Drazen, 'Registry research and medical privacy', *New England Journal of Medicine* 2004/350 afl. 14, p. 1452–1453. Ook OECD (2013) o.c.

79 M.R. Andersen & H.H. Storm, 'Cancer registration, public health and the reform of the european data protection framework: abandoning or improving european public health research?', *European Journal of Cancer* 2013/51 afl. 9, p. 1028–1038.

80 Een verstandig arts wees mij er eens op dat 'gb' opgetekend in het toenmalige papieren dossier van de postoperatieve follow-up van een patiënt niet alleen kon duiden op 'geen bijzonderheden' maar ook op 'geen belangstelling'.

medische gegevens dienen objectief te zijn, gebaseerd op de professionele standaard. Die standaard is gebaseerd op hetgeen van voorafgaande patiënten is geleerd en zowel via de wetenschap en al dan niet uitgewerkt in richtlijnen als praktische ervaring ter beschikking van de hulpverlener staat.
Via een wat andere weg dan Faden et al.[81] leiden beide uitgangspunten tot mijn conclusie[82] dat de patiënt die profiteert van solidaire, best mogelijke zorg volgens de huidige standaarden, een ethische verantwoordelijkheid heeft om aan een lerend zorgsysteem bij te dragen indien bepaalde voorwaarden zijn vervuld.

5.4 Anderen dan de patiënt

Voor hulpverleners, zorgaanbieders en zorgverzekeraars behoeft die verantwoordelijkheid minder toelichting. Los van de verantwoordelijkheid jegens patiënten en burgers om zo goed mogelijke zorg te bieden en bedreigingen voor de gezondheid af te wenden, die inherent aan het vak zou moeten zijn, is men ingebed in dat stelsel en wordt met publieke middelen betaald, waaronder ook het ontvangen van patiëntgegevens voor het 'primaire' doel. Men kan zich daarbij niet op een soort 'eigendomsrecht' op die gegevens beroepen.[83] Het verschil is wel dat van patiënten wordt gevraagd iets toe te laten: de gegevensverwerking ten behoeve van een lerend zorgsysteem gebeurt op de achtergrond en interfereert niet met de behandeling, terwijl van de andere partijen soms een actieve bijdrage wordt gevraagd.
De voorbeelden uit de vorige paragraaf laten zien dat die bijdrage ook wordt geleverd. Of werd geleverd want sinds de eerdergenoemde DIS-uitspraak van de AP lijkt er wel een zekere verkramping te zijn opgetreden. Veel van de eerdere verwerkingen ten behoeve van een lerend zorgsysteem waren gebaseerd op de – overigens naar mijn mening onjuiste – 'consent or anonymise'-benadering. En dan ging men aan de anonymise-kant zitten met, om toch gegevens uit verschillende bronnen te kunnen combineren, 'pseudonimisering' tussen bron en doelbestand, een weg die nu afgesneden lijkt.
Tijd om nader op de classificatie van gegevens in te gaan.

---

81 Faden (2013), o.c.

82 Zoals ook in E.B. van Veen, *Patient data for health research*, Den Haag: MedLawconsult, 2011, par. 10.5 http://www.medlaw.nl/wp-content/uploads/2016/05/11-patient-data-for-health-research.pdf.

83 Zie hfdst. 9 in I. Stirbu-Wagner et al., *Haalbaarheidsstudie indicatoren huisartsenzorg en etalage+-gegevens*, NIVEL, Utrecht, 2011, http://www.nivel.nl/sites/default/files/bestanden/Rapport-haalbaarheidsstudie-indicatoren-huisartsenzorg.pdf.

6 Anoniem, persoonsgegevens, gepseudonimiseerd, hoe zit het nu?

6.1 Vooraf

Een persoonsgegeven is elk gegeven dat betrekking heeft op een geïdentificeerde of identificeerbare natuurlijke persoon.[84] Onder de AVG verandert deze definitie niet, maar wordt toegevoegd aan de hand van welke elementen een persoon identificeerbaar is. Van het tegenovergestelde, anonieme gegevens, wordt geen definitie gegeven. Wel is er sinds oktober 2016 een belangrijke uitspraak van het Hof van Justitie EU waarop ik nog terugkom.
Het is thans alles of niets. Op persoonsgegevens is de Wbp (en de WGBO) van toepassing en met ingang van 25 mei 2018 de AVG en de UAVG. Op niet-persoonsgegevens is niets van toepassing. Die zijn vrij. Mede om die reden stelde de Article 29 Working Party[85] in een opinie uit 2007[86] dat het begrip persoonsgegevens ruim diende te worden uitgelegd. Toezicht zou dan mogelijk blijven. Ietwat optimistisch werd ook gesteld dat de nationale wetgeving voldoende nuanceringen laat om daarbinnen dan legitieme doelen van de gegevensverwerking te kunnen realiseren. Voor de doelen van een lerend zorgsysteem ontbreken in veel landen die nuanceringen en dus wordt daar uitgeweken naar de anonymise-benadering.
In 2014 bracht de Artikel 29-werkgroep een opinie uit over anonimiseringstechnieken.[87] De kern is dat de anonimisering volledig onomkeerbaar moet zijn. Het resultaat moet verwerking van persoonsgegevens voorgoed onmogelijk maken.

6.2 De AP over de DIS-data

Aansluitend op Opinie 4/2014 onderzocht de AP het DIS. Bij de zorgaanbieder wordt het BSN van de patiënt gepseudonimiseerd. De DBC-gegevens gaan vervolgens naar de NZa. De pseudonimisering is niet volledig onomkeerbaar, het CBS heeft een sleutel terug. Dat was een van de redenen voor de AP om in tegenstelling tot eerdere uitspraken[88] ook bij andere afnemers de aangeleverde gegevens als persoonsgegevens aan te merken, zoals de NZa, waar deze gegevens primair worden aangeleverd.

---

84 Art. 1 onder a Wbp.
85 Dit is een werkgroep samengesteld uit de nationale privacytoezichthouders ingesteld op grond van art. 29 Richtlijn 95/46/EC.
86 Opinion 2007/4 on the concept of personal data.
87 Opinie 5/2014.
88 CBP z2005-0814, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/uit/z2005-0882.pdf; CBP z2006-1382, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/uit/z2006-1382.pdf en CBP z2008-00292, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/med/med_20090616_cvz.pdf.

Een tweede reden is dat door de zorgaanbieder een intern koppelnummer wordt meegeleverd. Indien door de NZa onregelmatigheden in de aangeleverde gegevensset worden ontdekt, kan de zorgaanbieder via dat koppelnummer terug naar de oorspronkelijke patiëntgegevens.
Opvallend in de uitspraak is dat eerst wordt gesteld 'niet kan worden uitgesloten (…) tot een persoon te herleiden zijn ' en vervolgens '*Ook* kijkend naar de middelen (…) die redelijkerwijs kunnen worden ingezet'. De klassieke opvatting is dat de vraag of herleiding al dan niet kan worden uitgesloten, wordt bepaald vanwege de middelen die redelijkerwijs kunnen worden ingezet. Die opvatting wordt bevestigd in de nu te bespreken uitspraak van het Hof van Justitie van de Europese Unie (HvJ EU).

6.3 Het HvJ EU over herleidbaarheid op 19 oktober 2016

Aan de orde was de vraag of zogenaamde dynamische internetadressen[89] persoonsgegevens zijn. Van een statisch internetadres had het Hof al eerder bepaald dat dit een persoonsgegeven betreft.[90] Een dynamisch internetadres is niet rechtstreeks identificeerbaar. Over de vraag of het voor de internetprovider identificeerbaar is, wordt in r.o. 46 in lijn met de conclusie van de AG opgemerkt (met mijn cursivering):

> 'dat is niet het geval indien de identificatie van de betrokkene *bij de wet verboden wordt* of in de praktijk ondoenlijk is, bijvoorbeeld omdat zij – gelet op de vereiste tijd, kosten en mankracht – een excessieve inspanning vergt, zodat het gevaar voor identificatie in werkelijkheid onbeduidend lijkt.'

Hier, noch in de conclusie, iets over de noodzaak van onomkeerbaarheid. Indien het dynamisch IP-adres wordt gezien als een pseudoniem, zou het zelfs omkeerbaar mogen zijn indien de identificatie bij wet is verboden.
Met betrekking tot het niet-gecursiveerde element in deze rechtsoverweging, na het 'of' wordt ook een iets lagere standaard bepaald dan het 'volstrekt' onmogelijk. Tegelijk moet worden opgemerkt dat de uitspraak vragen openlaat. De mogelijkheden tot herleiding worden hier toegespitst op de internetprovider. Of iemand al dan niet herleidbaar is, wordt evenwel niet bepaald door dit relatieve criterium, namelijk degene die rechtmatig over de gegevens beschikt, maar op grond van een objectieve standaard 'wie dan ook', zoals het Hof eerder in de uitspraak zelf ook opmerkt.
In dat verband blijft de drempel om van anonieme gegevens te spreken hoog. Onder een veilig pseudoniem (dat niet gekraakt kan worden of herleid mag wor-

89 Bij elk bezoek aan het internet maakt men gebruik van een IP-adres. Bij dynamische internetadressen is dat telkens een ander adres dat willekeurig wordt toegewezen.
90 In zaak C-70/10, ECLI:EU:C:2011:771.

den) hangen de gegevens. Voor de vraag of het praktisch doenlijk is te herleiden moet niet worden uitgegaan van de jurist maar een slim statisticus. Voor die persoon is met behulp van andere openbare bronnen herleiding van ten minste een deel van de betrokkenen in de dataset wel mogelijk.[91]
Het 'bij wet verboden' levert ook complexe vragen op. Pogingen tot herleiding worden, als ik het goed zie, in het algemeen niet verboden[92] maar als die pogingen er vervolgens toe leiden dat men over persoonsgegevens beschikt, moet men wel een grondslag hebben om die te verwerken. Die grondslag zal vaak ontbreken. Bij het 'bij wet verboden' is voorts de vraag of daartoe ook voldoende is dat het verboden is om aan herleiding mee te werken, met name door het beroepsgeheim. Dan zou een veel grotere groep gegevens die nu als indirect identificerende gelden als anonieme kunnen worden aangemerkt, tenzij het anderszins praktisch doenlijk is om te herleiden.[93] Zo ver wil ook ik niet gaan.
Wat daarvan zij, de uitspraak laat zien dat indien het de internetprovider bij wet verboden was om het dynamisch IP-adres te herleiden en het tevens niet doenlijk zou zijn geweest, dat IP-adres geen persoonsgegeven zou zijn geweest. In de Duitse casus was het overigens niet bij wet verboden.

6.4 Gepseudonimiseerde gegevens in de AVG

In de AVG is een definitie van pseudonimisering opgenomen.[94] De bepaling is nogal complex maar komt er in essentie op neer dat het gaat om de verwerking van persoonsgegevens waarbij de gegevens waarmee de betrokkene kan worden

---

91 Borking wijst daar in diens achtergrondstudie bij het RVZ-advies over Patiënteninformatie terecht op, Borking Consultancy, 'Ongedolven goud: van data naar info', Wassenaar, 7 april 2014.

92 Tenzij dit gepaard zou gaan met een in art. 138a Sr (computervredebreuk) verboden gedraging dan wel het in strijd met het doelbindingsbeginsel (art. 9 Wbp) combineren van persoonsgegevens waarover men wel rechtmatig mag beschikken.

93 De kwestie heeft indertijd gespeeld bij de registratie van huisartsgegevens door het NIVEL ten behoeve van onderzoek naar verrichtingen in de huisartsenpraktijk, het LINH. De patiënten waren daar onder het lokale huisartsennummer opgenomen. Het NIVEL ging ervan uit dat daarmee een anonieme dataset werd verkregen. Men mocht op grond van de arbeidsovereenkomst niet herleiden en de huisartspraktijk mocht op grond van het (afgeleid) beroepsgeheim ook niet aan zo'n herleiding meewerken. Het CBP concludeerde echter dat het om persoonsgegevens ging. Overigens werd geaccepteerd dat het NIVEL deze gegevens wel op basis van een goed aangekleed geen-bezwaarsysteem mocht verwerken. College bescherming persoonsgegevens, *Onderzoek landelijke zorgregistraties, Rapport 3*, Den Haag: Cbp 2005. https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rapporten/rap_2005_zorgregistraties.pdf.

94 Art. 4 onder 5.

geïdentificeerd apart worden bewaard en er technische en organisatorische maatregelen zijn getroffen om te vorkomen dat deze persoonsgegevens (via die identificerende gegevens) toch aan de persoon worden gekoppeld.
De bepaling heeft, al dan niet in combinatie met meergenoemde NZa-uitspraak van de AP, het misverstand opgeroepen dat alle gepseudonimiseerde gegevens nu persoonsgegevens zijn geworden. Zoals ook blijkt uit de overwegingen (met name 26 en 29 waar pseudonimisering betrekking heeft op dezelfde verwerkingsverantwoordelijke en niet op de inschakeling van een *trusted third party* (TTP)), staat er echter niet meer dan dat pseudonimisering betrekking heeft op persoonsgegevens en dat deze techniek hun als zodanig niet die status ontneemt. Pseudonimisering is hier een door de verantwoordelijke omkeerbare bewerking.[95] Er bestaat ook pseudonimisering die niet door verantwoordelijke omkeerbaar is en anonieme gegevens kan opleveren mits aan een aantal additionele voorwaarden is voldaan. Mede op basis van de in noot 88 genoemde uitspraken van het CBP is in het verleden veel gegevensuitwisseling voor het onderhoud van het zorgstelsel of wetenschappelijk onderzoek daarop gebaseerd.
Ploem stelde overigens al voor het nieuwe artikel in de AVG dat alle gecodeerde gegevens per definitie persoonsgegevens zijn[96] waarbij schrijver dezes dan bij het 'anders' wordt genoemd. Hoewel correct, was dat te veel eer. Voor het anders had moeten worden verwezen naar de eerdergenoemde uitspraken van het CBP.
Gecodeerd- of gepseudonimiseerd-anoniem blijft dus een bestaanbare categorie al is het begrip gepseudonimiseerd nu wel 'gekaapt' voor een bepaalde vorm van pseudonimisering die steeds persoonsgegevens betreft. Voor de andere vormen zullen dan andere termen moeten worden bedacht. Hoe dan ook bepaalt AVG zeker niet het tegendeel, namelijk dat anonieme gegevens door pseudonimisering alsnog altijd persoonsgegevens worden. Al kan dan combinatie van gepseudonimiseerd-anonieme gegevens in het doelbestand uiteraard wel weer indirect identificerende gegevens onder het pseudoniem opleveren. Dat staat echter los van de terminologische verheldering.

6.5 Conclusie bij deze paragraaf

De voormelde uitspraak van het HvJ EU leidt tot een genuanceerder benadering over de grens tussen persoonsgegevens en anonieme gegevens dan de 'alles of niets'-benadering van de AP in diens nogal apodictische NZa-uitspraak. Gepseudonimiseerd- of gecodeerd-anonieme gegevens is bij de genuanceerde benadering een bestaanbare categorie, al liggen de grenzen nauw. De drempel om van anonieme gegevens te kunnen spreken (al dan niet gepseudonimiseerd of gecodeerd) blijft erg hoog en de hele keten van de bron van de gegevens via inter-

95 Zie ook: *Kamerstukken I* 2015/16, 33169, nr. AF.
96 M.C. Ploem, 'Gegeven voor de wetenschap', in: Vereniging voor Gezondheidsrecht, *Wetenschappelijk onderzoek in de zorg*, Den Haag: Sdu Uitgevers, 2010, p. 117–206, op p.137.

mediaire stappen tot het uiteindelijke doelbestand moet daarbij worden betrokken. Deze nuanceringen zijn van belang maar leiden af van waar het werkelijk om gaat, namelijk hoe kunnen en mogen gegevens veilig worden verwerkt voor een lerend zorgsysteem. De 'consent or anonymise'-benadering waarbij de nuanceringen dan in die tweede optie passen, biedt daarop geen antwoord. Er blijven vage grenzen en daarmee onzekerheid voor de praktijk en de toezichthouder. Voorts doet de consentoptie geen recht aan andere mechanismen dan consent om veilig persoonsgegevens voor een lerend zorgsysteem te mogen verwerken en de uitgangspunten waarom dat zou moeten. De anoniem-optie gaat eraan voorbij dat men die mechanismen ook op dat type gegevens van toepassing zou willen laten zijn.

7 Hoe verder

7.1 De veiligheid van gegevens

In plaats van al dan niet anoniem moet de vraag zijn of de gegevens al dan niet veilig zijn. De (patiënt)gegevens mogen uitsluitend worden gebruikt binnen die cirkel van een lerend zorgsysteem. De gegevens van een bepaalde patiënt eerder in het proces zullen niet mogen worden gebruikt voor besluiten later op basis van die gegevens omtrent diezelfde patiënt.[97,98]

Het gaat hier tenslotte, net als bij wetenschappelijk onderzoek, om het onderkennen van patronen, niet om personen. Ook al zullen die personen om valide gegevens over patronen te verkrijgen in eerste instantie uniek moeten kunnen worden onderscheiden, er is om die reden geen sprake van 'singling out' in de zin van de AVG.

Alle mij bekende dataplatforms waarbinnen patiëntgegevens voor een lerend zorgsysteem worden verwerkt voldoen inmiddels aan NEN Norm 7510 en/of ISO 27001. De vraag is of dat voldoende is. In het eind 2016 door AP gepubliceerde overzicht van datalekken kwam de zorg relatief het meest voor,[99] terwijl daar al geruime tijd volgens NEN Norm 7510 moet worden gewerkt.[100]

---

97 Deze ingewikkelde formulering omdat op basis van de in de tekst genoemde patronen de hulpverlening wel zal kunnen worden aangepast, maar dan voor alle patiënten die behoren tot de in het patroon onderkende categorie.

98 Tenzij bij de analyse een 'bevinding' blijkt waarvan de hulpverlener op de hoogte moet worden gesteld, zoals dat de patiënt – tenzij sprake is van een invoerfout in het EPD of HIS, hetgeen ook kan voorkomen – op een verkeerd medicijn is ingesteld. Dit voorbeeld uit de praktijk is overigens uitsluitend relevant bij bepaalde bewerkers die ook uitdrukkelijk die rol is toegekend.

99 https://autoriteitpersoonsgegevens.nl/nl/nieuws/1-jaar-meldplicht-datalekken.

100 Namelijk op grond van art. 2 van de Regeling gebruik burgerservicenummer in de zorg, *Stcrt.* 2008, nr. 105, p. 59 en het inwerkingtredingsbesluit (*Stb.* 2008, 186) op 1 juni 2008.

Bij hergebruik van patiëntgegevens is het in zoverre gemakkelijker om datalekken te voorkomen dat niet al die vele processen met losse applicaties en devices nodig zijn om de gegevens in eerste instantie te verkrijgen en evenmin de contacten met patiënten met de 'ouderwets schriftelijke' of elektronische interfaces van dien. Datalekken blijken juist daar voor te komen. Het gaat hier om een relatief gesloten omgeving met een beperkt aantal ingangen voor de gegevens en anonieme output.
Daarop aansluitend wordt in het project Eenvormige Toetsing, waarover zo direct meer, uiterst scherpe normen aangelegd, namelijk uitsluitend werken binnen een beveiligde omgeving (geen eventueel te stelen laptops met daarop patiëntgegevens[101]), via twee-factorauthenticatie.[102] Ook moet steeds een 'audit trail' op de gegevens mogelijk zijn.
Ik betwijfel of '(tweeweg)pseudonimisering' aan de bron voor deze veiligheid altijd noodzakelijk is, zoals gesteld door PBLQ in de context van wetenschappelijk onderzoek.[103] Dit temeer daar die pseudonimisering veelal niet door de zorgaanbieder zelf wordt verricht maar dat daarvoor ook weer een derde partij wordt ingeschakeld. Uiteraard gelden steeds de beginselen van noodzakelijkheid en proportionaliteit in samenhang met de in artikel 25 AVG genoemde uitgangspunten. Pseudonimisering kan evenwel na binnenkomst via een beveiligde verbinding ook bij de bewerker plaatsvinden. Overigens spreken wij dan eerder van encryptie. Het zal er in dat kader van afhangen wat van die bewerker wordt verwacht. Fungeert die tevens als een 'business intelligence'-omgeving voor de zorgaanbieder dan is meer heen-en-weerverkeer nodig naar de oorspronkelijke patiëntgegevens van de zorgaanbieder dan via pseudonimisering via een derde partij mogelijk blijkt. Dat geldt eens te meer indien die bewerker ook een rol speelt bij de primaire kwaliteitsborging van de patiëntenzorg (vergelijk het in noot 98 genoemde voorbeeld).
Is het doelbestand geen bewerker maar een nieuwe verantwoordelijke, dan lijkt mij dat pseudonimisering aan de bron, al dan niet met tussenschakeling van een derde partij, wel moet plaatsvinden.
Genuanceerde benaderingen zijn dus mogelijk en noodzakelijk binnen de voornoemde uitgangspunten van veiligheid volgens de ISO 27001-standaard en de artikel 25 AVG-uitgangspunten.

---

101 Zie http://www.rtvnoord.nl/nieuws/172113/Datalek-bij-UMCG-gegevens-van-1-300-patienten-op-straat.

102 Zie het zogenaamde moederdocument, module 12 op www.eenvormigetoetsing.nl.

103 T. Hooghiemstra et al., *Onderzoek naar de beveiliging van patiëntgegevens*, Den Haag: PBLQ, 2016.

7.2 Een regeling voor de kwaliteitsregistraties

De kwaliteitsregistraties kunnen worden begrepen als een van de instrumenten om de verwerking in het algemeen belang op het gebied van de volksgezondheid mogelijk te maken, zoals bepaald in artikel 9 tweede lid onder i van de AVG. Dit artikel maakt een uitzondering op het toestemmingsbeginsel.
Deze bepaling moet worden uitgewerkt in nationaal recht. Bij artikel 25 van de ontwerp-UAVG is dat naar mijn mening te rudimentair gebeurd. Met het tweede lid kan worden ingestemd. Dat bepaalt dat indien persoonsgegevens voor dit doel worden verwerkt, allen die bevoegd zijn tot de toegang tot deze gegevens moeten zijn onderworpen aan een geheimhoudingsplicht. De toepassing van *privacy enhancing technologies* wordt in deze bepaling terecht niet genoemd want volgt al uit artikel 25 AVG dat direct werkt. Het eerste lid laat naar mijn mening echter te veel ruimte. Op geen enkele wijze wordt benoemd welke verantwoordelijken deze doelen om welke redenen mogen inroepen, zoals dat bij artikel 21 Wbp (23 in de UAVG) wel het geval is. Hier zou een brede omschrijving moeten worden opgenomen van het type verantwoordelijken en verwijzing naar een ministeriële regeling waar nader wordt bepaald welke dit zijn en waar men zich aan moet houden. Zeer waarschijnlijk is daar bij de reacties op de internetconsultatie op teruggekomen[104] en voor een alternatief zij kortheidshalve verwezen naar de desbetreffende webpagina.[105]

7.3 Algemeen belang

In de AVG wordt het begrip algemeen belang maar liefst 73 maal genoemd. In de UAVG komt het voor in voornoemd artikel 25 en artikel 27, dat gelijk is aan het huidige artikel 23 tweede lid Wbp. Het feit dat het onderzoek in het algemeen belang is, is dan een van de criteria om ten behoeve van het onderzoek zonder uitdrukkelijke toestemming bijzondere persoonsgegevens te mogen verwerken. Net zoals dat begrip in artikel 7:458 BW een van de criteria is om door de hulpverlener zonder toestemming van de patiënt ten behoeve van het onderzoek patiëntgegevens te verstrekken.
Grip krijgen op de inhoud van het begrip algemeen belang is lastig. Algemeen of publiek belang kan in tweeërlei context worden gebruikt. In de eerste plaats als oriëntatie voor de politieke besluitvorming.[106] In die zin ook het SER-advies over overheid en markt. De oriëntatie wordt daar niet geoperationaliseerd: 'Het is uiteindelijk aan de democratisch gelegitimeerde organen van de politiek om de

104 Op het moment dat dit hoofdstuk werd afgesloten bereidde schrijver dezes een dergelijke reactie voor.
105 De lezer zal dan moeten zoeken onder afgesloten consultaties.
106 Uitsluitend de thans helaas verdwenen Tegenpartij van Koot en de Bie was unverfrohren voor het eigenbelang.

publieke belangen te bepalen'.[107] Die operationalisering vindt men dan meer in de politieke geschriften waar algemeen belang dan met name wordt afgezet tegen een 'neoliberale' ordening.[108]

Dat helpt ons hier niet verder want thans is een andere context van 'algemeen belang' aan de orde, namelijk als ijkpunt om van de algemene regels af te wijken.[109] Een operationalisering ontbreekt echter grotendeels. Bij de totstandkoming van de WGBO is het begrip algemeen belang in de context van het toenmalige artikel 1653m (na een nota van wijziging[110] het huidige 7:458 BW) slechts sporadisch aan de orde geweest. Onderzoek in verband met een louter commercieel of industrieel belang viel er niet onder. Evenmin onderzoek dat niet naar verwachting aan nieuwe wetenschappelijke inzichten zal kunnen bijdragen. Ook werd genoemd dat 'een groep van enige omvang naar verwachting aanzienlijk baat van het onderzoek zal kunnen hebben'.[111] Voor de volledigheid zij opgemerkt dat artikel 7:458 BW met een grote sprong in de tijd school heeft gemaakt in de WMO 2015 en de Jeugdwet zonder dat daarbij over deze bepalingen[112] in het parlement is gediscussieerd.

De politieke filosofie leert ons iets over het algemeen belang en vooral wat het niet is. Namelijk niet hetgeen in het belang is van de meerderheid, hoe verder ook gedefinieerd.[113]

Hier construeer ik het algemeen belang op de volgende twee pijlers.

1. Het algemeen belang betekent bescherming, via de in 2 genoemde pijler, tegen onvoldoende kwaliteit of gezondheidsbescherming van de kwetsbaren, wie dezen ook mogen zijn. Het betekent niet de beste gezondheidzorg of gezondheidsbescherming voor de meesten. Een lerend zorgsysteem is daarmee nog

---

107 Sociaal-Economische Raad, *Overheid én markt: Het resultaat telt!*, Den Haag: Sociaal-Economische Raad 2010, p. 36.

108 Bijv. R. Kuiper, *De terugkeer van het algemeen belang*, Amsterdam: Van Gennep 2014 en D. Marquand, *The decline of the public: The Hollowing out of citizenship*, Cambridge: Wiley, John & Sons 2004.

109 Overigens speelt het in deze context soms ook in het economisch ordeningsrecht een rol, namelijk bij diensten van algemeen economisch belang in de zin van art. 106 e.v. van het Verdrag betreffende de werking van de Europese Unie. Maar dan wordt die aanwijzing bepaald door de democratische organen als bedoeld in het SER-rapport, met overigens uiteindelijk eventueel een toetsing door het HvJ EU. In de tekst is aan de orde dat het ijkpunt lager is gelegd, namelijk bij private partijen.

110 *Kamerstukken II* 1993/94, 21561, nr. 286.

111 *Kamerstukken II* 1991/92, 21561, nr. 11, p. 47.

112 Resp. de art. 5.3.6 lid 2 onder a WMO 2015 en 7.3.12 lid 2 onder a Jeugdwet.

113 V. Held, *The public interest and individual interests*, New York: Basic Books, 1971 en M. Feintuck, *The public interest' in regulation*, Oxford: Oxford University Press, 2004.

wel in het belang van elke burger of patiënt omdat wij niet tevoren kunnen weten wie daarvan zal kunnen profiteren. Het kan enkelen betreffen.[114]

2. De uitkomsten van de analyses en de onderliggende gegevens dienen een openbare discussie over individuele hulpverlening, de inrichting van het stelsel en arrangementen voor gezondheidsbescherming. Dat heeft een aantal consequenties voor de kwaliteit van het onderzoek en de (wetenschappelijke) integriteit van degenen die de gegevens mogen verwerken[115] en beschikbaarheid van de gegevens volgens de FAIR-beginselen[116] die hier niet verder kunnen worden uitgewerkt. Van groter belang is dat algemeen belang hier in de context wordt geplaatst van een open democratische samenleving waar bijdragen aan de publieke discussie haast zonder uitzondering in het algemeen belang moeten worden geacht, zoals dat ook voor de pers geldt.[117]

Dit zijn nogal brede pijlers, die inderdaad verder kunnen worden uitgewerkt. Daarvoor is hier geen ruimte.
Tussen uitkomsten van gegevensverwerking ten behoeve van een lerend zorgsysteem en de aanpassing van werkwijzen, op welk niveau dan ook, liggen meerdere stappen. Daarover wordt niet uitsluitend binnen het lerend zorgsysteem beslist. Voor de grotere aanpassingen, anders dan bijvoorbeeld de protocollen binnen een zorgaanbieder of de algemeen geldende richtlijnen, gaat het om een publieke discussie en uiteindelijk besluiten volgens democratische procedures die in de democratische rechtstaat bij de rechter kunnen worden uitgedaagd. De twee pijlers staan als het ware op dat fundament.
Binnen zo'n bredere en relatief veilige, hoewel van vele kanten uitgedaagde, omgeving ben ik dan minder bezorgd om de overigens behartigenswaardige opmerking van C.H.F Polak in 1950: 'Waar elk recht aanstonds moet wijken voor het algemeen belang, daar is spoedig van recht geen sprake meer en lijdt de gemeenschap op den duur onherstelbare schade.'[118]

7.4 De burgerservicenummer(BSN-)kwestie

De vraag is waarop die aan het unieke onderscheidend kenmerk (teneinde tot valide uitkomsten te kunnen komen) mag worden gebaseerd waaraan de kwaliteits- of onderzoeksgegevens zijn opgehangen.

---

114 Aan zogenaamde weesziekten werd bij de totstandkoming van de WGBO niet gedacht. Daarover bijvoorbeeld http://www.nfu.nl/patientenzorg/complexezorg/zeldzame-ziekten/.

115 Zie: https://www.knaw.nl/nl/thematisch/ethiek/wetenschappelijke-integriteit.

116 Zie o.a.: http://www.dtls.nl/fair-data.

117 Zie ook art. 41 van de UAVG en de relatief uitvoerige motivering bij dit artikel.

118 C.H.F. Polak, Het begrip 'algemeen belang' in de verschillende onderdelen van het administratieve recht, *Preadvies VAR*, Haarlem: H.D. Tjeenk Willink & zoon, 1950, p. 50-51.

Binnen de zorg, het primaire proces, dient het onderscheidend kenmerk het BSN te zijn.[119] Indien ervan wordt uitgegaan dat kwaliteitsborging ook tot het primaire proces behoort, en de Wkkgz geeft daartoe alle reden, zou dat ook voor de kwaliteitsregistraties gelden (met inachtneming van het in de vorige paragraaf gestelde). Op grond van artikel 24 Wbp mag het dan niet voor andere leerdoelen van het lerend zorgsysteem. Dat betekent een enorme beperking. Eerder heeft schrijver dezes samen met Dirk de Jong ervoor gepleit dat eenweg[120] pseudonimisering van het BSN buiten het verbod van artikel 24 valt.[121] Ik wil niet ontkennen dat die redenering kwetsbaar is. En bovendien gaat zij niet op voor tweeweg pseudonimisering.[122]
Anders dan Dute heeft gesteld[123] is gebruik van het BSN vanuit het wetenschappelijk onderzoek niet uitsluitend bepleit vanuit een oogpunt van efficiency en betrouwbaarheid. Gebruik van het BSN of een op het BSN gebaseerd pseudoniem (de voorkeursoptie inderdaad) levert ietwat paradoxaal ook een privacy enhancing technology op. Betrouwbaarheid staat inderdaad voorop. En dan blijkt dat zonder BSN (pseudoniem) men veel dieper in de direct identificerende persoonsgegevens moet dan met. In die zin is een wetgevingsadvies van de AP inzake de pseudonimiseringsmaatregelen rond het aanbieden door commerciële partijen van elektronische onderwijsmiddelen hoogst merkwaardig. De privacy van kinderen en ouders is daarbij op diverse manieren precair en de regering en Tweede Kamer hebben daarover een fors aantal stukken uitgewisseld.[124] Uiteraard kan hier niet op de details worden ingegaan. Het voorlopige sluitstuk is een voorstel van de regering om voor de gegevensuitwisseling tussen school/leerling en de diverse elektronische toetsen en onderwijsmiddelen, het persoonsgebonden onderwijsnummer (= het BSN) te pseudonimiseren, waarbij voor verschillende doelen ook verschillende pseudoniemen zouden moeten worden gegenereerd. De AP stelt kritische vragen bij dit voorstel en meent dat: '(voor- en/of achter)naam en de groep van een onderwijsdeelnemer zullen evenwel meestal al voldoende zijn om een digitaal leermiddel aan de onderwijsdeelnemer van een onderwijsinstelling te kunnen koppelen'.[125] Of dat nu waar is of niet, die gegevens zouden de aanbieders van die leermiddelen nu juist niet hoeven te weten. En als het waar is, betekent dat dus unieke identificatie van de kinderen aan de hand van die ken-

119 Wet gebruik burgerservicenummer in de zorg. Wanneer het preadvies wordt gepubliceerd zal deze waarschijnlijk heten de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, *Stb*. 2016, 373.
120 M.a.w. er is geen sleutel terug.
121 De Jong en Partners plus MedLawconsult, Memo aan Zorg TTP van 14 juni 2013.
122 Dus wel een sleutel terug.
123 H.J.J. Leenen, J.C.J. Dute, W.R. Kastelein, *Handboek Gezondheidsrecht, deel II, gezondheidszorg en recht*, Bohn Staleu van Lochum, Houten, 2008, par. 5.2.8.
124 Zie *Kamerstukken II* nr. 32034.
125 AP 26 oktober 2016, Advies wetsvoorstel pseudonimisering, Z2016-14321.

merken en valt niet in te zien waarom dit alternatief het door de AP gevreesde koppelen zou kunnen voorkomen.
Ook met betrekking tot het gebruik van het BSN voor kwaliteitsregistraties en wetenschappelijk onderzoek zal het AP niet welwillend worden ontvangen. Het CBP verklaarde zich in een scriptieachtig wetgevingsadvies[126] tegen het gebruik van het BSN door Sanquin en de NCDR.[127] Volgens dat advies zou geen van beide organisaties het BSN mogen verwerken. Gelukkig heeft de regering de veiligheid van de bloedtransfusieketen zwaarder laten wegen. Voor de NCDR was in 2011 een sluitende registratie van cardiovasculaire implantaten nog een brug te ver. Na 2016, het 'jaar van de transparantie', zou men voor kwaliteitsregistraties de aarzelingen moeten laten varen. Voor de vraag welke kwaliteitsregistraties het BSN mogen verwerken kan worden aangesloten bij de in sectie 7.2 geschetste afbakening.
Voor wetenschappelijk onderzoek zal nog een langere weg te gaan zijn, waarvoor ik overigens wel pleit. Dat de apocalyptische visoenen van het CBP/AP bij ruimer gebruik van het BSN (binnen de in de vorige sectie beschreven voorwaarden) niet opgaan, blijkt overigens uit de Scandinavische landen waar het BSN al geruime tijd voor deze doelen mag worden verwerkt.
Inderdaad wordt via een (gepseudonimiseerd) BSN koppelen makkelijker. Ongelimiteerd koppelen wordt onder meer voorkomen door de volgende waarborg.

7.5 Toetsing

Hier spelen de volgende 'toetsingsmomenten'. Het eerste is welke kwaliteitsregistraties gebruik mogen maken van de in deze paragraaf geschetste uitzonderingen (geen toestemming en wel BSN). Het tweede is hoe zij daarvan gebruik mogen maken. Het derde toetsingsmoment is verdere ontsluiting (of uit de kwaliteitsregistraties of direct uit de EPD's dan wel de gegevens waarover zorgverzekeraars beschikken) ten behoeve van wetenschappelijk onderzoek.
Het eerste toetsingsmoment heb ik al in paragraaf 7.2 globaal geschetst. Het tweede toetsingsmoment valt naar mijn mening in twee elementen uiteen. Vooraf door een 'gegevensbeschermingseffectbeoordeling' (voorheen PIA)[128] in de zin van artikel 35 AVG. Continu door de 'privacycommissie' die in het reglement van de kwaliteitsregistratie moet worden ingesteld. Die commissie mag overigens ook een andere naam hebben, het gaat om de samenstelling en bevoegdheden, zoals uiteengezet in het project Eenvormige Toetsing (1T).[129] Dit project beoogt

126 CBP Advies conceptwijziging Besluit gebruik BSN in de zorg, Z2011-00063.
127 De kwaliteitsregistratie van (bepaalde) cardiovasculaire implantaten en de daarmee gemoeide ingrepen (ook hier is langetermijnfollow-up van de patiënt uiteraard van belang over verschillende zorgaanbieders), zie www.ncdr.nl.
128 Privacyimpactassessment. Een standaardafkorting voor de gegevensbeschermingseffectbeoordeling ben ik nog niet tegengekomen. Mijn voorstel is: GBE.
129 Zie www.eenvormigetoetsing.nl.

toetsing te realiseren voor alle observationeel gezondheidsonderzoek in Nederland. Ploem pleitte eerder voor dergelijke toetsing[130] die echter om alle partijen mee te krijgen en dubbele toetsing te voorkomen nog niet zo makkelijk te realiseren is. De bij 1T beschreven samenstelling en bevoegdheden zijn toegesneden op het beoordelen van wetenschappelijk onderzoek. Dat is het derde toetsingsmoment. Alle kwaliteitsregistraties lenen zich voor vrijgeven van de daar bijeengebrachte gegevens voor wetenschappelijk onderzoek en dienen dus zo'n 'toetsingscommissie' te installeren. Voor het monitoren van de kwaliteitsregistratie zelf (blijft deze binnen de doelstelling en opzet volgens de GBE), zullen ook andere partijen in de 'privacycommissie' zitting kunnen nemen.
Bij het derde toetsingsmoment, voordat wetenschappelijk onderzoek met gegevens mag plaatsvinden, gaat het zowel om de wetenschappelijke meerwaarde als om de opzet en uitvoering in het licht van de te beschermen belangen van de betrokkenen. Voor de toetsingscriteria – op dit moment in wording – zij verwezen naar de in noot 129 genoemde site.

7.6 Governance

Het begrip governance kan vele betekenissen hebben afhankelijk van de context maar een scherpe definiëring ontbreekt. Dat is waarschijnlijk de reden dat het zo regelmatig als een bezweringsformule in de discussie opduikt. Organiseer 'governance' en het zit wel goed.[131] Er bestaat evenwel nogal een verschil tussen 'governance' door de wetgever of bestuursorganen van bepaalde maatschappelijke activiteiten[132] en 'governance' door private actoren van de activiteiten waar zij zelf voor staan, zoals bij de Governance Code Zorg.[133] In beide gevallen gaat het wel over besturen en dan een bepaalde wijze van besturen, namelijk minder verticaal, meer transparant en om verantwoording, ook via informele processen. Bij governance *door* private of semi-actoren is het speelveld uiteraard beperkt door de governance *van* hen door wetgever/bestuursorganen. De paragrafen 7.1 tot en met 7.4 handelden over governance van het lerend zorgsysteem. In paragraaf 7.5 was governance door het veld aan de orde want de toetsing zal worden gebaseerd op zelfregulering.[134] Die toetsing is daarmee een van de elementen van de governance door. De elementen kunnen hier niet worden uitgewerkt. Bij eerdergenoemd project 1T worden in de zogenaamde modules diverse elementen van

130 Ploem (2010), o.c. nt. 96.
131 Bijv. het project kwaliteitsregistraties noemt 'governance' als een van de ijkpunten zonder te omschrijven wat governance inhoudt.
132 Daarover o.a. A.M. Kjær, *Governance*, Cambridge: Polity Press 2004.
133 https://www.brancheorganisatieszorg.nl/nieuws_list/667/#more-667.
134 En de wijze waarop wordt geprobeerd dit te realiseren veronderstelt als zodanig weer een governancemodel.

'good research governance' benoemd[135] en voor kwaliteitsregistraties gelden die evenzeer. Een van de elementen is het betrekken van relevante patiëntenorganisaties. Over hoe dat succesvol kan, bestaat in de context van wetenschappelijk onderzoek inmiddels veel materiaal.[136]
Overigens gaat het om een evenwicht van belangen. Zoals beschreven in paragraaf 4 zijn veel kwaliteitsregistraties ontstaan vanuit betrokken artsen en haakten de ziekenhuizen pas later aan, 'nolens volens' soms. Het zwaartepunt lijkt nu naar de ziekenhuizen te verschuiven mede omdat de bureaus van de betrokken koepels, de NVZ en NFU, voor het vervolg van de discussie beter geëquipeerd lijken dan aan het eind van een verlengde werkdag in de Domus Medica, het hoofdkwartier van de FMS, vergaderende artsen. En hoewel wildgroei en hobbyisme bij kwaliteitsregistraties niet mogen voorkomen, zou het eveneens zonde zijn om het enthousiasme en de vaak bij de koepels onbekende en soms ook ongemakkelijke praktijkkennis van de professionals te verliezen.

7.7 Consent revisited

Voor toestemming is bij de opname in kwaliteitsregistraties geen plaats. Dan kunnen zij net zo goed worden afgeschaft want zij worden volstrekt onbetrouwbaar. Voor zover mij bekend heeft niemand tot nu toe ook gepleit voor opname in kwaliteitsregistraties uitsluitend op basis van consent maar mogelijk was niet iedereen er zich van bewust dat vrij lang in de keten bijzondere persoonsgegevens worden verwerkt.
Bij (verder) ontsluiten voor wetenschappelijk onderzoek van in verband met de zorg verzamelde patiëntgegevens (dus niet extra gegevens) bestaat een serieus discussiepunt. De defaultsituatie is volgens de huidige wetgeving toestemming. Die wetgeving ging van de volgende omstandigheden niet uit.

- Zulke ontsluiting moet niet als de uitzondering worden gezien maar als noodzakelijk voor een lerend zorgsysteem.
- Die ontsluiting is met de komst van EPD-systemen makkelijker mogelijk geworden met daarbij tussenschakeling van 'privacy by design'-technieken;
- Waar voorheen nog kon worden volgehouden dat gegevens als anoniem konden worden aangemerkt, gaat dat nu niet meer op. Genuanceerd onderzoek maakt gebruik van persoonsgegevens, ook al blijven de NAW van de betrokkenen gemaskeerd.

---

135 Zie voor een eerste aanzet E.B. van Veen, 'Obstacles to European research projects with data and tissue: solutions and further challenges', *EJC* 2008, 44 (10), p. 1438-1450 en meer uitgewerkt O'Doherty KC et al., 'From consent to institutions: designing adaptive governance for genomic biobanks.' *Soc Sci Med* 2011, 73(3) p. 367-374.

136 Voor een overzicht zie: M. de Wit et al., 'Voorwaarden voor succesvolle betrokkenheid van patiënten/cliënten bij medisch wetenschappelijk onderzoek', *TSG*, 3/2016, p. 91-100.

– Het betreft gegevens die volgens een op maximale veiligheid ingerichte definitie niet als anoniem kunnen worden aangemerkt (en inderdaad niet als 'open data' kunnen worden vrijgegeven) maar binnen een veilige omgeving voor de onderzoeker anoniem zijn.

Dan kan men ervoor pleiten om veel meer op de consentoptie terug te vallen of meer op de uitzondering, dus artikel 7:458 BW voor de verstrekker, artikel 23 tweede lid Wbp (thans) voor de verantwoordelijke samen met thans artikel 8 onder f Wbp (de restgrondslag). Onder de AVG zal artikel 6 onder e naar mijn mening geschikter zijn: 'de gegevensverwerking is noodzakelijk voor een taak van algemeen belang'.

Het zal niet verbazen dat de tweede optie mij liever is. Ik moge verwijzen naar de beschouwing in paragraaf 6 maar eveneens naar de in deze paragraaf beschreven waarborgen. Die gelden over de hele line, met of zonder consent.

8 Slotopmerkingen

Dit hoofdstuk kent twee samenhangende verhaallijnen. De eerste is de zo objectief mogelijke beschrijving van hoe het lerend zorgsysteem thans werkt, inclusief het normatieve kader. Dat kan op zich al vragen oproepen maar de tweede verhaallijn is meer contentieus. Die is samenvattend als volgt. Een lerend zorgsysteem is noodzakelijk niet uitsluitend om de kwaliteit over de hele linie te verbeteren volgens de bestaande standaarden, maar ook om bestaande standaarden ter discussie te kunnen stellen, of het nu gaat om die binnen de zorg, of meer op mesoniveau de inrichting van het zorgstelsel of meer macro, dat van gezondheidsbescherming. Patiëntgegevens liggen ten grondslag aan dat leerproces net zoals deze patiëntgegevens het gevolg zijn van eerder leren. De privacy van de patiënten dient te worden geborgd doordat deze gegevens uitsluitend binnen de cyclus van schema 1 worden verwerkt. Onder die omstandigheden en gelet op de morele grondslagen van een solidair zorgstelsel en mits binnen de voorwaarden van de vorige paragraaf, zou toestemming van de patiënt geen rol van betekenis moeten spelen.

Uiteraard is dit geen gemakkelijke boodschap. Ik behandel tot slot twee mogelijke tegenwerpingen. De eerste komt uit een discussie of consent voor observationeel (bigdata)onderzoek inderdaad tot bias leidt. Mark Rothstein dacht van niet.[137] Het aardige van dit special issue van de *American Journal of Bioethcis* was dat de reacties ook werden gepubliceerd. Een aantal andere reacties toont dat consent wel degelijk tot bias leidt. Ik bespreek hier het commentaar van Ioannidis die het volgende stelt. Inderdaad kan door consent wel degelijk bias ontstaan, al zijn er ook statistische technieken om daarvoor te compenseren maar die observationele studies voldoen toch al niet aan diens voorwaarden voor goed wetenschappelijk onderzoek. Voorts stelt Ioannidis dat – samenvattend – het openbaren

137 M.A. Rothstein & A. B. Shoben, 'Does consent bias research?', *American Journal of Bioethics* 13(4) 2013, p. 27–37.

(disclosing) van dit soort informatie negatieve consequenties kan hebben voor de betrokkenen.[138] Daarover het volgende. Inderdaad lijkt mij dat observationeel gezondheidsonderzoek via hergebruik beperkingen heeft. Daarom ook de toetsing die ook een methodologische beoordeling moet omvatten. Indien met openbaren niet is bedoeld dat de onderzoeker kennisneemt van de NAW van de betrokkenen, hetgeen namelijk ook niet de bedoeling is indien wel met informed consent onderzoek wordt verricht, doelt Ioannidis dan kennelijk op een 'groepsprivacy'-argument. Dit argument gaat eraan voorbij dat de huidige ordening een momentopname is en mogelijk bepaalde andere groepen juist in een nadelige positie brengt. Voor wat acceptabel is en wat niet hebben wij nu juist gegevens nodig die de discussie daarover kunnen voeden. Overigens ben ik op de naar mijn mening onhoudbaarheid van het 'groepsprivacy'-argument elders uitvoerig ingegaan en kortheidshalve zij daarnaar verwezen.[139]

De tweede tegenwerping is dat het via 'apps' gemakkelijk is om toestemming te verkrijgen. Bijvoorbeeld het voorstel om in de 'wachtkamer' tablets beschikbaar te hebben waarop 'nader gebruik' wordt uitgelegd waar men dan al dan niet mee kan instemmen.[140] Ik heb inmiddels de leeftijd om iets meer dan gemiddeld een ziekenhuis te bezoeken maar hoef daar zelden te wachten. *Die* kwaliteitsverbetering heeft bij mijn ziekenhuis kennelijk gewerkt. Maar uiteraard zijn er nieuwe mogelijkheden om patiënten te bereiken en toestemming voor 'nader gebruik' te verkrijgen, bijvoorbeeld een link bij de afspraakbevestiging.

Transparantie is een van de voorwaarden van de governance en daarin zou een systeem van attenderen op 'nader gebruik' via links na een afspraak goed passen. Of dat moet leiden tot een dergelijk consentmechanisme is evenwel een andere vraag. Met Sethi en Laurie[141] stel ik vraagtekens bij wat door hen is genoemd de 'fetishisation of consent'. Waar informed consent voor is bedoeld, namelijk het eigen leven zoveel mogelijk vorm te kunnen geven, is hier niet van toepassing. Wel hoe gezamenlijk als een gemeenschap, met verantwoordelijken tegenover elkaar, kan worden bijgedragen aan kansen op verbetering voor nog onbekenden via een open discussie dankzij cijfers over wie mogelijk niet de beste vorm van zorg of gezondheidsbescherming ontvangt. Er zijn overigens ook nogal wat aanwijzingen dat ook patiënten dit belang onderkennen.[142]

---

138 J.P.A. Ioannidis, 'Informed Consent, Big Data, and the Oxymoron of Research That Is Not Research', *American Journal of Bioethics*, 13:4 2013, p. 40-42.

139 Van Veen 2011, sectie 10.6.5.

140 Voor 'nader gebruik' lichaamsmateriaal zie: https://www.bbmri.nl/wp-content/uploads/2016/12/Health-RRI-25-11-2016-Corrette-Ploem-en-J%C3%B6rg-Hamann-naar-toestemming-voor-nader-gebruik-in-het-AMC.pdf.

141 Sethi en Laurie (2013), p. 174.

142 R. Coppen et al., 'Hergebruik van medische gegevens voor onderzoek; wat vindt de Nederlander van het toestemmingsvereiste', *NTvG* 2016;160:A9868, zie ook de presentatie van Lydia Makaroff, directeur van de European Coalition of Cancer Patients, dia nr. 9, op http://www.iscintelligence.com/archivos_subidos/ecpc_gdpr.pdf.

Literatuur

Andersen en Storm (2013)
M.R. Andersen & H.H. Storm, 'Cancer registration, public health and the reform of the european data protection framework: abandoning or improving european public health research?', *European Journal of Cancer* 2013/51 afl. 9, p. 1028–1038.

Beauchamp en Childress (2013)
T.L. Beauchamp & J.F. Childress, *Principles of biomedical ethics*, New York: Oxford University Press 2013.

Citteur en Rijken (2013)
J.M.E. Citteur & J.J. Rijken, 'Verstrekken van patiëntengegevens door zorgaanbieders aan zorgverzekeraars', *TvGR* 2013/37 afl. 8, p. 750-763.

Coppen et al. (2016)
R. Coppen et al., 'Hergebruik van medische gegevens voor onderzoek; wat vindt de Nederlander van het toestemmingsvereiste', *NTvG* 2016;160:A9868.

Dute (2008)
J. Dute, 'De Wet publieke gezondheid', *TvGR*, 2008/32, afl. 8, p. 576-591.

Faden et al. (2013)
R.R. Faden et al., 'An ethics framework for a learning health care system: a departure from traditional research ethics and clinical ethics', *Hastings Center Report 43/s1* 2013.

Feintuck (2004)
M. Feintuck, *The public interest' in regulation*, Oxford: Oxford University Press, 2004.

Held (1971)
V. Held, *The public interest and individual interests*, New York: Basic Books, 1971.

Hooghiemstra et al. (2016)
T. Hooghiemstra et al., *Onderzoek naar de beveiliging van patiëntgegevens*, Den Haag: PBLQ, 2016.

Ingelfinger en Drazen (2004)
J.R. Ingelfinger & J.M. Drazen, 'Registry research and medical privacy', *New England Journal of Medicine* 2004/350 afl. 14, p. 1452–1453.

Ioannidis (2013)
J.P.A. Ioannidis, 'Informed Consent, Big Data, and the Oxymoron of Research That Is Not Research', *American Journal of Bioethics*, 13:4 2013, p. 40-42.

Kuchinke et al. (2014)
W. Kuchinke et al., 'A standardised graphic method for describing data privacy frameworks in primary care research using a flexible zone model', *International Journal of Medical Informatics* 2014/83 afl. 12, p. 941–957.

Leenen, Dute en Kastelein (2008)
H.J.J. Leenen, J.C.J. Dute, W.R. Kastelein, *Handboek Gezondheidsrecht, deel II, gezondheidszorg en recht*, Bohn Staleu van Lochum, Houten, 2008.

Levi en Bos (2015)
M. Levi, W. Bos, 'Weinig keuzebereidheid bij patiënten', *NTvG* 2015:159 (3).

Moerel (2014)
E.M.L. Moerel, *Big data protection: How to make the draft EU regulation on data protection future proof*, Tilburg: Tilburg University 2014.

Moerel en Prins (2016)
E.M.L. Moerel & J.E.J. Prins 'Privacy voor de homo digitalis', in: Nederlandse Juristen-Vereniging, *Homo Digitalis*, Amsterdam: Wolters-Kluwer 2016, p. 1–136.

Van der Nat (2016)
Paul van der Nat, 'Value based health care gedijt bij Hollandse cultuur van transparantie', *Skipr*, https://www.skipr.nl/blogs/id2899-value-based-healthcare-gedijt-bij-hollandse-cultuur-van-transparantie.html 31 oktober 2016.

OECD (2013)
OECD, *Strengthening health information infrastructure for health care quality governance good practices, new opportunities and data privacy protection challenge: OECD health policy studies*, Paris: Organization for Economic Co-operation and Development (OECD) 2013.

Olsen et al. (2007)
L. Olsen et al., *The learning healthcare system: Workshop summary (IOM roundtable on evidence-based medicine)*, Washington, DC: National Academies Press 2007.

Ploem (2010)
M.C. Ploem, 'Gegeven voor de wetenschap', in: Vereniging voor Gezondheidsrecht, *Wetenschappelijk onderzoek in de zorg*, Den Haag: Sdu Uitgevers, 2010.

Polak (1950)
C.H.F. Polak, 'Het begrip 'algemeen belang' in de verschillende onderdelen van het administratieve recht', *Preadvies VAR*, Haarlem: H.D. Tjeenk Willink & zoon, 1950.

Porter (2009)
M.E. Porter, 'A Strategy for Health Care Reform — Toward a Value-Based System', *N Engl J Med* 2009; 361:109-112.

Rebers et al. (2016)
S. Rebers et al., 'A randomised controlled trial of consent procedures for the use of residual tissues for medical research: preferences of and implications for patients, research and clinical practice', *PLOS ONE* 2016/11 afl. 3.

Rothstein en Shoben (2013)
M.A. Rothstein, & A. B. Shoben, 'Does consent bias research?', *American Journal of Bioethics* 13(4) 2013, p. 27–37.

Sethi en Laurie (2013)
N. Sethi & G. Laurie, 'Delivering proportionate governance in the era of eHealth: Making linkage and privacy work together', *Medical Law International* 2013, Vol 13(2-3) p. 168–204.

Sociaal-Economische Raad (2010)
Sociaal-Economische Raad, *Overheid én markt: Het resultaat telt!*, Den Haag: Sociaal-Economische Raad 2010.

Stirbu-Wagner et al. (2011)
I. Stirbu-Wagner et al., *Haalbaarheidsstudie indicatoren huisartsenzorg en etalage+-gegevens*, NIVEL, Utrecht, 2011.

Van Veen (2011)
E.B. van Veen, *Patient data for health research*, Den Haag: MedLawconsult, 2011.

Van den Wijngaard et al. (2011)
C.C. Van den Wijngaard et al., 'In search of hidden q-fever outbreaks: linking syndromic hospital clusters to infected goat farms', *Epidemiology and Infection* 2011/139 afl. 01, p. 19–26.

Deel 3
Big data en zorginstellingen

Deel 3B
De juridische uitdagingen voor een zorginstelling bij big data

Mr. T.G. Kleefman*

* Tinga Kleefman is bedrijfsjurist IE, ICT en Privacy bij UMC Utrecht.

1 Inleiding

Een zorginstelling heeft in haar dagelijkse praktijk op vele gebieden te maken met de uitwisseling van data. De door de zorginstelling verzamelde data worden uitgewisseld met andere zorgverleners zodra de zorg wordt overgedragen. Bij gezamenlijk onderzoek van verscheidene zorginstellingen worden eveneens klinische data met elkaar gedeeld. Het (beter) toegankelijk maken van verzamelde data biedt daarbij meer mogelijkheden tot het doen van onderzoek. Subsidieverlenende instellingen stellen steeds vaker als voorwaarde dat de data openbaar toegankelijk zijn. Daarbij wordt educatie meer en meer digitaal verleend, waardoor ook onderzoek met die data kan worden uitgevoerd.

Traditioneel verzamelt de zorgverlener de data omtrent de gezondheid en het welzijn van een patiënt op het moment dat deze de patiënt in zijn spreekkamer spreekt. Inmiddels vindt er een verschuiving plaats in het zorgproces; patiënten kunnen thuis en voorafgaand aan het bezoek hun medische gegevens verzamelen en met de zorgverlener delen. Dankzij ontwikkelingen op het gebied van toepassingen van het gebruik van *mobile devices* is er een sterk groeiende markt op het gebied van instrumenten waardoor het mogelijk is om continu patiëntendata te verzamelen.

De patiënt heeft er behoefte aan om data over zijn eigen gezondheid en welzijn te kunnen verzamelen. Zodra van veel personen medische gegevens digitaal beschikbaar en doorzoekbaar zijn gemaakt, kunnen door vergelijking van de gegevens afkomstig van meerdere patiënten, resultaten met elkaar worden vergeleken. Als gevolg van de vergelijking kan zorg beter op de specifieke kenmerken van een patiënt worden toegepast (*personalized medicine).*
Een softwareapplicatie te gebruiken op mobiele apparaten wordt hierna aangeduid met 'app'. Op het gebied van gezondheid zijn er vele apps die zaken als beweging en voeding kunnen meten. Te denken valt aan stappentellers, calorietellers en hardloopapps. Er zijn ook apps die de gebruiker in staat stellen om zijn gebruik van medicijnen bij te houden. In de zorg is er tevens behoefte aan een app die meerdere aspecten van de gezondheid meet aan de hand waarvan een patiënt deskundig en verantwoord advies ontvangt. Vele commerciële apps blijken in de praktijk onvoldoende precies en volledig te zijn om op basis van de daarin verzamelde data verantwoord advies te kunnen geven. Zorginstellingen zijn daarom in toenemende mate betrokken bij de ontwikkeling van apps. In dit artikel worden apps die op elektronische wijze de gezondheid monitoren en begeleiden aangeduid met 'eHealth-apps'.

In de praktijk zijn zorginstellingen steeds vaker actief bij de ontwikkelingen van eHealth-apps. Dit vereist specifieke kennis van het intellectueel-eigendomsrecht, het ICT-recht, het privacyrecht en het ontwikkelproces van dergelijke apps. Het ontwikkelproces van een app is bijzonder; de functionaliteiten, de inhoud en de

mogelijkheden omtrent gebruik van de data zijn veelal niet bepaald bij aangaan van de samenwerking. Dit betekent dat het proces van onderhandeling creatief en flexibel verloopt. De structuur en de inhoud van de contracten zullen hiermee rekening moeten houden.

Het centrale thema van deze bijdrage aan het preadvies vormt het begrip 'big data'. Hierna ga ik in op de relevantie van de term 'big data' voor het geven van juridisch advies aan een zorginstelling. Daarna schets ik kort het kader van relevante wet- en regelgeving. Vervolgens zal het praktische kader waarbinnen het delen door en ontvangen van data van een zorginstelling van en met anderen worden uiteengezet. Voorts zal worden ingegaan op de verschillende juridische instrumenten bij het maken van afspraken over het verzamelen en gebruiken van (big) data. Daarbij ga ik in op de te maken afspraken op het gebied van het intellectueel eigendom bij de ontwikkeling van eHealth-apps in de overeenkomsten tussen de zorgverlener en de bouwer van de app. Ook ga ik kort in op een service level agreement, een specifieke contractvorm in de ICT. De bewerkersovereenkomst bespreek ik uitgebreider. Ter illustratie zet ik de juridische uitdagingen van het laten ontwikkelen van een eHealth-app uiteen. Bij wijze van handvat is een juridische checklist opgenomen.

2 Big data

Allereerst ga ik in op het begrip big data. Voor mij is de betekenis van het te maken onderscheid tussen 'data' en 'big data' van geringe invloed op het geven van juridisch advies. Per situatie zullen de afspraken omtrent het verzamelen en delen van data moeten worden beoordeeld. Daarbij is van belang met welk type partijen de data worden gedeeld, welke data worden gedeeld, waar de data worden beheerd, door wie en onder welke voorwaarden (door derden) de data kunnen worden gebruikt. Of de verzamelde data ook aan definities van 'big data' zouden beantwoorden is daarbij voor mij van ondergeschikt belang. Een exacte opgave van welke data worden verzameld en gedeeld en of deze direct of indirect herleidbaar zijn tot de persoon is wel van groot belang. Dan dienen deze data aan de privacywet- en regelgeving te worden getoetst. De grootte van een verzameling data of de mogelijke koppelingen met andere bestanden en welke entiteiten daar gebruik van kunnen maken hebben zeker hun weerslag op te treffen technische voorzieningen en te gebruiken juridische instrumenten. Het juridisch advies zal namelijk verschillen naar mate de data extern van de zorginstelling worden beheerd en er bij de uitvoering commerciële partijen zijn betrokken. In de praktijk worden grote verzamelingen data in verband met de technische capaciteit en mogelijkheden bij voorkeur door anderen dan de zorginstelling verwerkt. Hoe meer (type) partijen bij de verzameling en het gebruik van persoonsgegevens betrokken zijn, hoe veelzijdiger het juridisch advies wordt. Hierna zal het accent liggen op het adviseren omtrent verzamelingen extern beheerde data.

3 Kader van wet- en regelgeving

Wet- en regelgeving stellen eisen aan de wijze waarop de privacy van de personen die de data betreffen, dient te worden beschermd. Mede gelet op de overige artikelen van dit preadvies ga ik hierna slechts kort in op de relevante wet- en regelgeving.

Zodra de data 'persoonsgegevens' in de zin van de Wet bescherming persoonsgegevens (Wbp) betreffen, dienen de afspraken aan dit wettelijk kader te worden getoetst. Een persoonsgegeven is op grond van artikel 1 sub a Wbp elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel tot deze persoon te herleiden is. Gegevens die betrekking hebben op overledenen of rechtspersonen, zijn geen persoonsgegevens als bedoeld in de onderhavige bepaling. Zodra deze gegevens echter eveneens betrekking hebben op nog levende, natuurlijke personen en indien zij mede bepalend kunnen zijn voor de wijze waarop deze personen in het maatschappelijk verkeer worden beoordeeld of behandeld, dan zijn zij wel weer een persoonsgegeven.[1] Een voorbeeld van data waarvan de privacy niet eindigt bij de dood van de persoon is de data vervat in een DNA-profiel.

In het kader van de medische gegevens vastgelegd in een medisch dossier is eveneens de Wet op de geneeskundige behandelingsovereenkomst (WGBO) relevant. Deze wet bevat bijvoorbeeld verplichtingen omtrent het houden en bewaren van een medisch dossier.

De Wbp en WGBO zijn naast elkaar van toepassing.

Op het gebied van bescherming van privacy geldt ook Europese regelgeving. Op dit moment is binnen Europa ook nog Richtlijn 95/46/EG van toepassing.[2] De Europese richtlijn is geïmplementeerd in de nationale wetgevingen van de lidstaten. Per 25 mei 2018 geldt Europese Verordening 2016/679.[3] De verordening betreft Europese regelgeving op het gebied van bescherming van personen in het kader van de verwerking van persoonsgegevens. Deze verordening is dan recht-

1 Wbp MvT, II, nr. 3, p. 47.

2 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

3 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

streeks van toepassing in alle EU-lidstaten. Desondanks hebben Europese lidstaten reeds nationale wetgeving en zullen de huidige nationale wetgevingen mogelijk (nader) op de Europese regelgeving worden aangepast. Aangezien voornoemde verordening al wel is vastgesteld, dient bij de advisering reeds met de toepassing daarvan rekening te worden gehouden. Een gemiddeld onderzoekstraject duurt immers meerdere jaren.

In het kader van de (technische) beveiliging van data is er in de vorm van zelfregulering een aantal normen geformuleerd. De in internationaal verband tot stand gekomen ISO 27001 formuleert de normen voor informatiebeveiliging van managementsystemen. Deze norm specificeert eisen voor de implementatie van beveiligingsmaatregelen die passen bij de behoefte van de betrokken organisatie. De ISO 27002 bevat geen normen maar beschrijft het proces van totstandkoming van de norm, namelijk door middel van een risicoanalyse en het vervolgens gezamenlijk vatstellen van de norm. Ten aanzien van de zorg kennen wij nog NEN 7510. Deze laatste is op basis van de voornoemde ISO-normen specifiek van toepassing op de Nederlandse gezondheidszorg.

In het kader van de rechten op de verzameling van data is eveneens de Databankenwet[4] of de Auteurswet[5] van toepassing.
Degene die het risico draagt van de voor (het aanleggen van) de databank te maken investering wordt als producent in de zin van de Databankenwet aangemerkt.[6] De producent heeft het uitsluitende recht om toestemming te verlenen voor – kort gezegd – het gebruik van de databank door anderen.[7] Als de data geschikt zijn tot het doen van onderzoek, is het derhalve primair de producent die de toegang tot het gebruik van de data kan verlenen. Deze rechten van de producent laten de rechten van anderen op (onderdelen van) de databank onverlet.[8] Die rechten kunnen derhalve de (contractueel bedongen) rechten van zorginstellingen zijn die eveneens aan de verzameling van de data hebben bijgedragen, maar ook de patiënten van wie de data afkomstig zijn.[9]

De software die gebruikt wordt bij het beheer van een eHealth-app is eveneens een recht van intellectueel eigendom. De Auteurswet is ter zake van toepassing.[10] De software voor zover weergegeven in de broncode en het voorbereidend mate-

4 Nationale wetgeving als gevolg van het implementeren van Richtlijn 96/9 van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken.
5 Art. 10 lid 3 Auteurswet.
6 Art. 1 sub b Databankenwet.
7 Art. 2 lid 1 Databankenwet.
8 Art. 2 lid 2 Databankenwet.
9 Hfdst. 6 Wbp, art. 35 e.v.
10 Art. 10 lid 1 onder 12 Auteurswet, alsmede art. 45h-45n Auteurswet.

riaal kunnen als werk worden aangemerkt, mits het oorspronkelijk is en de *stempel van de maker* draagt.[11] De grafische vormgeving en de tekstuele bijdragen kunnen eveneens als werk in de zin van de Auteurswet worden aangemerkt.[12] Het mogen gebruiken van software, tekst en foto's is afhankelijk van de toestemming van de maker ervan. Met de makers van de onderdelen van een eHealth-app dienen daarom afspraken te worden gemaakt. Hiertoe kan een licentieovereenkomst worden afgesloten waarin de toestemming voor het gebruik wordt gespecificeerd en de condities waaronder worden vastgelegd.

In deze bijdrage ligt niet de nadruk op de uitleg en toepassing van de relevante regelgeving, maar wel op de praktische toepassing ervan.

4 Toepassingsgebied van big data binnen de zorginstelling

De taken van een zorginstelling kunnen in drie pijlers worden onderverdeeld, te weten zorg, onderzoek en educatie. Het aandeel van de dienstverlening vallend binnen de verscheidene pijlers verschilt naar mate de taken van de zorginstelling verschillend zijn. Zo rust op een publiekrechtelijke instelling als een academisch ziekenhuis een wettelijke verplichting om academisch onderwijs te geven en verricht zij op grote schaal wetenschappelijk onderzoek. Bij een huisartsenpraktijk zal het aandeel onderzoek en educatie geringer van omvang zijn. Welke invulling de zorginstelling aan de drie pijlers ook geeft, de instelling zal op elk gebied met de verzameling en dus bescherming van data te maken krijgen.

4.1 Educatie

Het aspect van big data in het kader van educatie is op zich een interessant onderwerp. Educatie wordt steeds meer gefaciliteerd door digitale communicatiemiddelen, zoals web-based onderwijs als examenfaciliteiten. Door het afnemen van vaardigheidstesten van personeel en studenten kunnen data worden verzameld waarop vergelijkend onderzoek kan worden verricht. In vergelijking met de pijlers van zorg en onderzoek is naar mijn mening bij educatie uitsluitend bijzonder dat er een afhankelijkheidsrelatie bestaat tussen de cursist en de aanbieder van onderwijs. Immers, in hoeverre is een student die zich heeft verbonden aan een universitaire studie vrij om extensief gebruik van zijn persoonsgegevens te weigeren? Hoe ver mag een werkgever gaan in onderzoek op persoonsgegevens afkomstig van zijn personeel? Belangrijke vragen, maar deze zullen binnen het kader van dit artikel niet worden uitgewerkt. De technische en juridische inrichting van een online educatieplatform verschilt – wat mij betreft – niet van hetgeen

11 HR 4 januari 1991, *NJ* 1991 Van Dale/Romme.
12 Art. 10 lid 1 onder 1, 6, 9 en 10 Auteurswet.

bij een eHealth-app noodzakelijk en vereist is. In het hiernavolgende zal ik mij beperken tot de gebieden van zorg en onderzoek in het kader van het gebruik van eHealth-apps.

4.2 Zorg

De wijze van zorgverlening kent een wijziging/verandering als gevolg van het gebruik van eHealth-apps. Het betreft bijvoorbeeld de persoon die data genereert, het tijdstip waarop en de duur waarvoor data worden verzameld, de locatie waar de data worden beheerd en het type zorg dat wordt verleend. Meer specifiek kunnen in een eHealth-app data worden geregistreerd afkomstig van de patiënt en vanuit zijn huis, worden verzonden naar een door de ICT-dienstverlener beheerde server, die het op zijn beurt ter beschikking stelt aan de zorgverlener opdat de data aan het elektronisch patiëntendossier (EPD) kunnen worden toegevoegd. Het EPD is vervolgens door de patiënt zelf, digitaal en buiten de spreekkamer van de zorgverlener inzichtelijk. De zorgverlener kan vervolgens zorg op afstand verlenen door de patiënt persoonlijk digitaal of telefonisch advies te geven. De patiënt kan zich daardoor ook beter geëquipeerd voelen in zijn hulpvraag naar zorg. Patiënten hebben daarnaast de behoefte hun data met meerdere partijen te kunnen delen, zoals het ziekenhuis, de huisarts of andere familieleden en scholen. Zo kan een eHealth-app ook de (mantel)zorgers faciliteren.
Welke data kunnen er worden gedeeld? Zowel patiënt als zorgverlener heeft er behoefte aan om gegevens over bijvoorbeeld gewicht, hartslag, beweging, medicijngebruik, pijn, vermoeidheid, et cetera voortdurend of regelmatig bij te houden. Door gebruik te maken van een eHealth-app kunnen cijfers worden verzameld. Ook kunnen via de eHealth-app interviews worden gehouden. Daarbij kan de zorgverlener in de app de patiënt van relevante, deskundige informatie en tips voorzien. De data betreffen persoonsgegevens, niet alleen doordat ze door de zorgverlener herleidbaar zijn naar de betrokken patiënt, maar ook door het gebruik van een mobile device en bijvoorbeeld het daaraan verbonden IP-nummer, het gebruikte wifinetwerk, het e-mailadres, telefoonnummer en dergelijke.

4.3 Onderzoek

Veel van de data-uitwisseling in de zorg vindt plaats in het kader van onderzoek. Onderzoek naar 1) kwaliteit van de zorginstelling; 2) onderzoek ter verbetering van zorg voor groepen patiënten; of 3) in het kader van specifieke patiënten ('personalized medicine'). De organisatie en het juridisch advies van data ten behoeve van kwaliteitsregistratiesystemen kosten de zorginstellingen en haar bedrijfsjuristen veel tijd. In deze publicatie zal dit verder niet worden uitgewerkt.

Bij onderzoek wordt veelal samengewerkt met meerdere partijen. Immers door de dataverzamelingen van meerdere partijen te combineren ontstaat er een interessante bodem voor onderzoek, zelfs mogelijk big data. Hierna zullen de wat mij

betreft belangrijkste juridische instrumenten bij het contracteren met de betrokken partijen in eHealth en verzamelingen van data worden besproken.

5 Juridische instrumenten

5.1 Desca-model

In de contracten worden afspraken gemaakt over de rechten ten aanzien van het gezamenlijk verzameld materiaal. Een veelgebruikte template bij onderzoek en binnen de academische wereld is het Desca-model.[13] De template en een uitgebreide toelichting ervan zijn via internet te downloaden. Dit model is veelal verplicht bij het maken van afspraken in het kader van door de Europese Commissie verleende subsidies, maar is ook geschikt voor de generieke afspraken inzake samenwerking. In het kader van het gebruik bij data-uitwisseling verwijs ik graag naar de artikelen met betrekking tot intellectueel-eigendomsrechten, kennis, resultaten van de samenwerking en de gebruiksrechten daarop. Bij het doen van onderzoek tussen – onder meer – academische partners versnelt het de onderhandeling over de afspraken indien van dit herkenbare model gebruik wordt gemaakt. In artikelen 8, 9 en 10 Desca zijn standaardbepalingen opgenomen over de rechten op hetgeen partijen als kennis, intellectueel eigendom, data, software en dergelijke inbrengen (background) en welke rechten van gebruik anderen daaraan kunnen ontlenen (access). De artikelen geven een kader waarin afspraken worden gemaakt over hetgeen gezamenlijk tijdens de samenwerking aan intellectueel eigendom wordt gegenereerd (foreground).

In het kader van een samenwerking op het gebied van een nieuwe eHealth-app kan worden opgenomen dat de tekstuele inhoud, inhoud van protocollen, mogelijke algoritmes en kennis van veilige marges bij de automatische verwerking van meetresultaten door de zorgverlener wordt ingebracht. Ook kan met de ICT-dienstverlener worden afgesproken dat de data die door het gebruik van de eHealth-app worden gegenereerd in hun onderlinge verhouding, uitsluitend aan de zorgverlener toekomen.

Het Desca-model biedt echter geen standaardbepalingen over de afspraken op het gebied van het waarborgen van de privacy van de bij de samenwerking betrokken persoonsgegevens, anders dan door een generieke geheimhoudingsbepaling.[14] Een bepaling omtrent geheimhouding alleen is onvoldoende. Het type afspraken dat plaatsvindt in het kader van de bescherming van persoonsgegevens zal hierna in paragraaf 5.4 Bewerkersovereenkomst worden uitgewerkt.

13 http://www.desca-2020.eu/.
14 Art. 10 Desca-model.

Vanzelfsprekend dient de overeenkomst afspraken te bevatten over het testen ervan. De afspraken over het testen zouden in de samenwerkingsovereenkomst kunnen worden opgenomen, maar het is ook niet ongebruikelijk om die op te nemen in de licentieovereenkomst (5.2) of SLA (5.3).

5.2 Licentieovereenkomst

Een zorginstelling maakt in de praktijk veelal gebruik van een externe ICT-dienstverlener voor het beheer van een dataverzameling. Zodra er met meerdere zorginstellingen voor eenzelfde onderzoek data worden verzameld, wordt daarvoor in de meeste situaties gebruikgemaakt van de diensten van een externe ICT-beheerder. Het is dan de ICT-onderneming die de data beheert, of nog door een derde (in een cloudoplossing) de data laat beheren. De wijze van aanlevering of het genereren van de data wordt in ICT aangeduid met de term SaaS (software as a service) of ASP (application service provided). In de overeenkomst omtrent de toegang tot de software (bij wijze van dienstverlening) worden de condities opgenomen waaronder de software kan worden opgenomen. Deze rechten op gebruik kunnen in een generieke overeenkomst van dienstverlening worden opgenomen, maar worden vaak ook met licentieovereenkomst aangeduid. In de overeenkomst wordt meestal bepaald dat de auteursrechten, reeds ontwikkeld door de ICT-partij voorafgaand aan de overeenkomst, eigendom zijn en blijven van de ICT-partij. Zodra voor een eHealth-app op het gebied van de software maatwerk wordt overeengekomen, kunnen partijen daarover afwijkende afspraken maken. In de algemene inkoopvoorwaarden van de Nederlandse Federatie van Universitair Medische Centra is opgenomen dat het intellectueel eigendom daarvan aan het UMC toekomt.[15] De kwaliteit en de kwantiteit van de gebruikers zullen in een licentieovereenkomst eveneens worden begrensd. Net als het doel waarvoor de software mag worden gebruikt. In de licentieovereenkomst kunnen ook de inbreng van de zorgverlener bij de ontwikkeling van de eHealth-app worden opgenomen en wat de ICT-partij daar op haar beurt wel en niet mee mag doen. De zorgverlener levert vaak de medische kennis en parameters. De rechten op de interfaces en afbeeldingen dient ook te worden geregeld. Zoals bij iedere ontwikkeling is het verstandig in de overeenkomst met de ICT-partij op te nemen over welke functionaliteiten de software dient te beschikken.

5.3 SLA

In een service level agreement worden de afspraken gemaakt over de beschikbaarheid van de web-based applicatie en de daarmee beheerde dataverzameling. De op te nemen afspraken betreffen voornamelijk de uitvoering en zijn over het algemeen van feitelijke en cijfermatige aard. Voorbeelden zijn: afspraken over

15 Art. 17 Algemene inkoopvoorwaarden van het UMC, versie 14 juli 2016.

wanneer de online applicatie beschikbaar komt, het percentage dat de app online beschikbaar is, wanneer onderhoud gepleegd mag worden, wanneer er een helpdesk kan worden geraadpleegd en hoe snel en op welke wijze er gereageerd dient te worden op hulpvragen en foutmeldingen. De functie van helpdesk kan ook, tezamen met de updates en upgrades van software, in een separate onderhoudsovereenkomst worden opgenomen. De locatie van de server en de entiteit die deze beheert is eveneens van groot belang voor de toepassing van het toepasselijk recht. Dit is met name van belang voor de bescherming van de privacy indien de locatie zich buiten de EU bevindt. In het kader van een helpdesk dient opnieuw de vraag te worden gesteld wie dit type van dienstverlening uitvoert, waar de betrokken personen zich bevinden en tot welke data zij toegang hebben bij het uitvoeren van hulpvragen. Indien de helpdesk ten aanzien van een eHealth-app zich buiten de zorginstelling bevindt, kan het verlenen van begeleiding door een helpdesk eveneens als een bewerking worden gezien zodra de helpdesk bijvoorbeeld de persoonsgegevens van de database kan inzien.

5.4 Bewerkersovereenkomst

Op grond van de geldende wet- en regelgeving dienen afspraken te worden gemaakt tussen de partij die het doel van en wijze waarop de data verwerkt gaan worden (mede) vaststelt.[16] De te maken afspraken zullen derhalve afspraken betreffen over het doel van de verzameling, het gebruik daarvan (door anderen), de locatie waar de data worden opgeslagen, door wie en hoe de data beveiligd worden. De afspraken hoeven niet anders te zijn wanneer het geanonimiseerde data betreft,[17] maar in het hierna volgende wordt ervan uitgegaan dat de data eveneens persoonsgegevens bevatten in de zin van de Wbp.

Om aan de eisen gesteld in de wet- en regelgeving op het gebied van de privacy te kunnen voldoen, is het van groot belang dat de te treffen technische en organisatorische oplossingen voldoende vertrouwen geven dat de risico's voldoende zijn beperkt. Het is derhalve zinvol dat op het gebied van de uitwisseling van data de bedrijfsjurist, de privacyfunctionaris en de ICT-afdeling van een zorginstelling met elkaar nauw samenwerken. Het waarborgen van privacy is immers niet uitsluitend een taak die bij de bedrijfsjurist ligt, maar dient een punt van aandacht voor de gehele zorginstelling te zijn. Elke discipline brengt immers zijn eigen deskundigheid met zich mee en daar waar de verscheidene disciplines de expertise en ervaring delen en elkaars jargon leren begrijpen, worden oplossingen

16 Hfdst. 2 Wbp, artikel 6 e.v.

17 Op anonieme data is de Wbp niet van toepassing. De data kunnen echter wel economische waarde vertegenwoordigen waardoor de verstrekker er belang bij heeft dat de data goed en juist beveiligd worden. Dat hoeft niet via een bewerkersovereenkomst, maar de afspraken zouden vergelijkbaar met een bewerkersovereenkomst kunnen worden beschreven.

gevonden die ook breed gedragen kunnen worden. Om de veiligheidsrisico's in kaart te kunnen brengen is een 'privacy impact assessment' (PIA) een handig en misschien wel noodzakelijk instrument. NOREA, de vereniging van IT-auditors biedt daarvoor een handig model.[18] Hoewel de risicoverdeling en de aansprakelijkheid juridisch goed geregeld dienen te worden, dient de privacy voornamelijk technisch en organisatorisch goed te zijn uitgewerkt.
Indien de zorginstelling besluit mee te doen aan een database die buiten de instelling wordt beheerd, is de zorginstelling op grond van de Wbp de 'verantwoordelijke', en diegene die de database beheert de 'bewerker'. In geval van onderzoek kan de instelling ook de rol van bewerker vervullen, indien deze ook voor anderen data verwerkt. In het hiernavolgende wordt ervan uitgegaan dat de bewerker een ICT-dienstverlener betreft.

Onder 'bewerkingen' wordt verstaan wanneer persoonsgegevens bijvoorbeeld worden:
– verzameld, vastgelegd en geordend;
– bewaard, bijgewerkt en gewijzigd;
– gedeeld met andere partijen;
– opgevraagd en geraadpleegd;
– gekoppeld aan andere databestanden;
– gewijzigd en vernietigd.

Er zijn verschillende modellen van bewerkersovereenkomsten op de markt. Zo is er het NVZ-model, en het model van de Vereniging Nederlandse Gemeenten. Deze laatste betreft een praktisch en compact document. Vaak hanteren bewerkers (de vorenbedoelde ICT-dienstverleners) een eigen model. In de bewerkersovereenkomst wordt het navolgende opgenomen.

De doelomschrijving beperkt de mogelijkheden van het bewerken van de data. Het is derhalve verstandig om dit in een zo vroeg mogelijk stadium te bepalen. Dit is een verplichte voorwaarde. Er dient te worden omschreven wat er met de data mag en dient te gebeuren. Indien meerdere partijen recht hebben op bijvoorbeeld toegang tot de data, dient dit reeds in de doelomschrijving te zijn opgenomen. Indien de database ten behoeve van onderzoek wordt gegenereerd, is het verstandig om de mogelijkheden van (toekomstig) gebruik nauw met de betrokken onderzoekers te bespreken. Het gebruik van de database wordt namelijk beperkt door de specifieke doelstelling. Het zijn immers ook de patiënten die aan de geformuleerde doelstelling hun toestemming verlenen.

Hoewel dit geen wettelijk voorschrift is, is het raadzaam om de lijst met de exacte data aan een bewerkersovereenkomst toe te voegen. Zeker bij het gebruik van een eHealth-app via een mobiel apparaat kan veel data door de ICT-dienstverle-

18 http://www.norea.nl/Norea/Actueel/Nieuws/PIA+nieuwe+versie.aspx.

ner worden verzameld over de wijze van gebruik, hoelang en op welk moment van de dag wordt gebruikt en welke pagina's worden geraadpleegd, waarbij de ICT-dienstverlener ook eigen commerciële belangen kan hebben. De data van een eHealth-app vertegenwoordigen (ook) een commerciële waarde voor de andere partijen. Het is daarom verstandig om (in de licentieovereenkomst) afspraken te maken over de mogelijkheden van het plaatsen van advertenties. Door het toevoegen van de lijst met te verwerken data, worden de rechten op de beschikbare data transparanter en onderwerp van gesprek tussen partijen.

In het geval van de beveiliging van de data zou ervan uit moeten worden gegaan dat de ICT-dienstverlener de specialist is met betrekking tot de mogelijkheden van beveiliging. Het is daarom te adviseren dat de ICT-dienstverlener aantoont welke maatregelen worden getroffen in het kader van de veiligheid van de data. De voornoemde PIA is daarvoor een handig instrument. Het is daarbij te adviseren dat de beschreven maatregelen worden getoetst en bij voorkeur door een derde. Een zorginstelling beschikt immers niet over de kennis en middelen om alle externe partijen zelf aan een IT-audit te onderwerpen. Goed om te weten dat de ICT-dienstverleners vaak al een derde een audit hebben laten uitvoeren en daardoor over een rapport van een deskundige en onafhankelijke derde beschikken. Deze zou als bijlage van de bewerkersovereenkomst kunnen worden opgenomen. Daarbij kan worden opgenomen dat men elk jaar een dergelijke audit laat doen en men verplicht is de getroffen maatregelen te handhaven, althans te verbeteren zodra dit redelijkerwijs op basis van de technische mogelijkheden wordt geadviseerd door de auditor.

6 Checklist eHealth-app

Tot slot geef ik een checklist ten behoeve van het geven van juridisch advies inzake de verzameling en bewerking van (big) data door een eHealth-app. De checklist is bedoeld als hulpmiddel bij het verkrijgen van inzage in de omvang van hetgeen juridisch afgesproken kan worden.

1. Welke data worden er verzameld? Geef een overzicht van alle datavelden.
2. Met welk doel worden de data verzameld?
3. Wie zijn de partijen die bij de verzameling zijn betrokken en welke rol vervullen zij?
4. Op welke locatie worden de app en de data beheerd?
5. Op welke wijze worden de data verzameld? Geef daarbij de datastroom weer.
6. In het geval dat de wijze een nieuw te ontwikkelen app betreft, hoe wordt die ontwikkeld en welke partijen zijn daarbij betrokken? Wie levert de software? Wie beheert de data? Wie levert de tekst? Wie hebben de afbeeldingen gemaakt?
7. Hoe ontvangt de zorgverlener de data die met behulp van de app worden gegenereerd? Hoe kunnen de data aan het EPD worden toegevoegd?

8. Welke andere partijen hebben toegang tot de data? Wie besluit of derden toegang tot de data kunnen krijgen?
9. Over welke functionaliteiten dient de app te beschikken?
10. Hoe en door wie worden potentiële gebruikers zoals patiënten benaderd?
11. Wie betaalt waarvoor?
12. Wat is de uitkomst van de privacy impact assessment?

Deel 4
Big data en wetenschappelijk onderzoek

Deel 4A
Big data en open science

PROF. DR. F. MIEDEMA

Deel 4B
Big data, medisch-wetenschappelijk onderzoek en gegevens-bescherming

MR. M. MOSTERT

Deel 4
Big data en wetenschappelijk onderzoek

Deel 4A
Big data en open science

Prof. dr. F. Miedema*

* Frank Miedema is sinds 2009 decaan en vicevoorzitter van de raad van bestuur van UMC Utrecht en is een van de initiatiefnemers van Science in Transition.

1 CUDOS

Niet alleen de Europese Unie (EU), maar ook de National Institutes of Health (NIH) en NWO hebben het concept Open Science omarmd. Staatsecretaris van OCW, Sander Dekker heeft tijdens het Nederlands voorzitterschap van de EU in april 2016 met de Amsterdam Call for Action on Open Science[1] een sterk signaal afgegeven. Binnen afzienbare tijd zal dit grote gevolgen hebben voor de onderzoekers en de instituten. Het gaat hier niet alleen om het zogenaamde open-access-beleid ten aanzien van wetenschappelijke publicaties, hetgeen, in eerste instantie en terecht, in de media de meeste aandacht heeft gekregen. Het vrij beschikbaar maken van publicaties zodra ze zijn gepubliceerd is geheel in lijn met de idee van wetenschappelijke kennis als 'public good', conform de klassieke wetenschapssociologie uit 1942 van Robert Merton (Merton 1973 en Miedema 2012).
Merton heeft een sociologie ontworpen en verder uitgewerkt tot in de vroege jaren zeventig van de vorige eeuw, die gebaseerd is op normatieve, wenselijke uitgangspunten zoals gemeenschappelijkheid, universalisme, belangeloosheid en georganiseerde scepsis. In het Engels is dit bekend geworden onder het acroniem CUDOS. Het delen van informatie en resultaten is inderdaad een essentieel onderdeel van de wetenschap en de internationale wetenschappelijke gemeenschap. De publicatiecultuur heeft zich dan ook in de laatste zestig jaar sterk ontwikkeld, mede doordat wetenschap als maatschappelijke activiteit in omvang gigantisch is toegenomen. Ook is er een toegenomen specialisatie binnen de disciplines geweest. Naast het delen van publicaties is ook het delen van gegevens, data, onderzoeksresultaten en materialen geheel in lijn met de idealen van Merton. Immers in het belang van de vooruitgang van de wetenschap is die beschikbaarheid van en toegang tot de meeste recente resultaten van collega-onderzoekers ('peers') van het grootste belang. Wetenschappers bouwen voort op het eerdere werk van collega's waar dan ook ter wereld, voegen daaraan toe, corrigeren zo snel en efficiënt elkaars fouten en dwalingen. Dit komt de gehele voortgang van de wetenschap en indirect de maatschappij ten goede. Veelal wordt hierbij gedacht aan de natuurwetenschappen en biomedische wetenschappen die universele concepten, wetten en kennis produceren die in principe overal ter wereld geldig zijn en kunnen worden toegepast. Voor de geneeskunde en gezondheidswetenschappen geldt dit meer voor de biomedische inzichten, maar minder of soms geheel niet voor de invloed van gedrag en omgevingsfactoren die vaak lokaal bepaald kunnen zijn, ook binnen de grenzen van landen en steden.
Voor ons denken over big data en het gebruik van big data voor biomedisch en gezondheidsonderzoek dat reeds grote vlucht genomen heeft, lijken de Mertoniaanse principes niet alleen zeer relevant, maar hebben ook een grote mate van urgentie. De zorg om 'healthy aging, healthy urban living, vital and smart cities'

1 https://www.eu2016.nl/documenten/rapporten/2016/04/04/amsterdam-call-for-action-on-open-science.

is groot. Een van de grote uitdagingen van deze tijd is immers gezondheid. Betaalbaar, betaalbaar voor iedereen en dus inclusief. En liefst zo persoonlijk mogelijk, passend bij genotype en fenotype zodat met maximale effectiviteit onnodige bijwerkingen worden vermeden. Het gaat in toenemende mate over preventie en publieke gezondheid naast de curatieve zorg waardoor de klassieke biomedici en 'health engineers' samen moeten werken met hun collega's uit de sociale en geesteswetenschappen maar ook met juristen, bestuurskundigen en economen.
Voor het begrip van en vervolgens de relevante interventies op de invloed van leefomgeving en milieu moeten ook sociaal geografen betrokken zijn. Veel innovatie in het domein van de gezondheid is farmaceutisch en biotechnisch gedreven, maar de keuze van de toepassing heeft sterke ethische en politieke aspecten. Immers: 'niet alles wat kan, moet'. Veel biotechnologische en ICT-producten of -methoden worden voor de toepassing en introductie niet of nauwelijks gevalideerd of blijken bij validatieonderzoek niet de resultaten te geven die werden verwacht. Dus ook medisch-ethici, 'science and technology'-onderzoekers en politieke filosofen moeten geëngageerd worden (Jasanof 2016).
Ongeacht de opinie over mogelijkheid of wenselijkheid van vraagsturing in de wetenschap is er een gemeenschappelijk gedragen wens dat wetenschappelijk onderzoek direct of indirect maatschappelijk nut zal hebben of heeft. Dat uitgangspunt, maar ook voor hen die wetenschap bedrijven puur als *l'art pour l'art*, versterkt de onderbouwing en de noodzaak van de toepassing van de Mertoniaanse gedragsregels. Dus is data delen, zowel van publicaties en ruwe onderzoeksgegevens en materialen verkregen uit grote langlopende cohortstudies essentieel voor het doen van het hedendaagse onderzoek. Dat onderzoek is erop gericht inzichten te verwerven waarmee anderen voort kunnen, maar die inzichten kunnen ook bijdragen aan de 'science for policy', het ontwerpen van het systeem van publieke gezondheid waar publiek, politiek en privaat bij elkaar komen.

2 Incentives and reward

Ondanks Merton's CUDOS en het feit dat er grote maatschappelijke uitdagingen aan de orde zijn en dat 'grand challenges' urgentie hebben, is de krachtige roep om open science weer actueel. Want de wetenschap als sociologisch systeem functioneert niet volgens de regels van Merton. Ze functioneerde zelfs maar in heel geringe mate ooit volgens de CUDOS-principes. Merton benadrukte, paradoxaal misschien, competitieve elementen in de wetenschap, zoals het belang van de prioriteit van een wetenschappelijke ontdekking en de eer die daaraan verbonden wordt. Ook liet hij zien hoe stratificatie in de wetenschap een rol speelt, dat er elitevorming is waar macht en invloed aan toegekend wordt en van uitgaat. Heel goede wetenschappers in een dergelijk systeem krijgen meer gedaan dan hun mindere collega's. Prioriteit gaat bijna altijd samen met geheimhouding en elites en hun macht vormen een potentiële bedreiging voor belangeloosheid en 'organized sceptisism'. Toen ook de levenswetenchappen *big science* werden,

waarvoor grote bedragen aan personeel en laboratoriumapparatuur en ICT-infrastructuur nodig zijn, werd de wetenschap zeer competitief. Toen er sinds de jaren zeventig van de vorige eeuw ook nog jaarlijks meer onderzoekers werden opgeleid dan er onderzoeksgeld beschikbaar was, is de hypercompetitie losgebarsten waar in we ons nu in de gehele wereld in bevinden. In die competitie wordt, ondanks sterke internationale tegengeluiden, de laatste dertig jaar vooral gestuurd op academische publicaties in zogenaamde 'high impact' tijdschriften, citaties, patenten en binnengebrachte onderzoeksubsidies uit bijvoorbeeld de EU. Alle actoren in het systeem van de hedendaagse academische wetenschap hebben hun karakteristieke rol; van junior onderzoeker, decaan, post-docs, promovendi, maatschappelijke organisaties en patiëntenorganisaties maar ook de kennistransferorganisaties en hun juridisch medewerkers. Ook de, wat we vroeger collectebusfondsen noemden, zoals Hartstichting, KWF en bijvoorbeeld de Nierstichting hebben in dit systeem lang meegedraaid. Als direct gevolg van de publicatiedrift hebben de tijdschriften heel goede zaken gedaan, hun bedrijven zijn sterk gegroeid en ze zijn voordelig eigenaar geworden van 'content' die door noeste onderzoekers werd gemaakt, opgeschreven, beoordeeld en gepubliceerd. Dat laatste deden ze om in dit systeem naar de volgende fase van hun loopbaan te komen. De krachtiger roep om uit dit verdienmodel te breken heeft in vele landen geklonken, ook sinds 2013 in Nederland.[2] Dit systeem is optimaal ingericht voor het maken van academische carrières, maar blijkt inefficiënt voor het maken van 'significant knowledge': robuuste kennis waarmee we de grote maatschappelijke uitdagingen kunnen beginnen te adresseren. Veel gepubliceerde data blijken minder bruikbaar of onvoldoende robuust en dat genereert nu al jarenlang, zoals *The Lancet* dat in januari 2014 in een editorial typeerde, 'research waste' die jaarlijks optelt tot enorme bedragen. Dat is verlies aan wetenschappelijke vooruitgang en dus ook tijdverlies bij het aanpakken van de maatschappelijke problemen.[3]

3 Open science en team science

Om in een dergelijk competitief systeem te werken en te kunnen blijven werken en carrière te maken zijn de principes van Merton niet behulpzaam. Wetenschappers sturen op de output die gevraagd wordt in de academie waarin het individu en haar resultaten worden beoordeeld. Het delen van met veel inzet verkregen kennis, databestanden, preliminaire resultaten, biomaterialen en MRI- of CT-beeldmateriaal verzwakt de positie van de gever, want helpt 'de ander ' aan snel en gemakkelijk verkregen gegevens. Het blijven zitten op met moeite verkregen ruwe data ook lang na de publicatie ervan was de norm en is helaas nog steeds wat we zien in het veld. Het is niet onlogisch, immers de data kunnen tot vol-

2 http://www.scienceintransition.nl.
3 http://www.thelancet.com/series/research.

gende artikelen leiden of misschien wel een reeks artikelen en dat is toch nog vaak de pasmunt voor de volgende stap in de academische carrière. Dagelijks starten onderzoekers dure klinische studies en cohortstudies waarbij patiënten en gezonde vrijwilligers belast worden met afname van bloed en onderzoeken om data te maken die elders al voorhanden zou zijn geweest, indien ze toegankelijk zouden zijn geweest.
Hoewel we naar buiten de mythe van excellente onderzoekers en hun competitie soms nog idealiseren, is er nu het breed gedeelde besef dat in de huidige tijd waarin complexe multidisciplinaire problemen ('real world problems') moeten worden opgelost, er ook andere wetenschap en wetenschappers nodig zijn (Nowotny 2015). Onderzoekers die kunnen en willen samenwerken, de relevante kennis willen delen, over de grenzen van de oude disciplines en faculteiten heen kunnen denken en die zich kunnen verhouden met burgers en politici die belanghebbenden zijn ten aanzien van maatschappelijke uitdagingen die internationaal zijn, maar vaak ook regionaal om een oplossing vragen. 'Think globally but act locally' is dus het motto. We zijn dus op zoek naar de team science.

Om dit te bereiken moeten we in transitie naar open science. Daarvoor is een fundamenteel ander 'incentive and reward'-systeem nodig. Een ander verdienmodel waarin onderzoekers beloond worden om in dit nieuwe systeem de juiste dingen op excellente wijze te doen. Onderzoekers moeten beloond worden voor het onmiddellijk delen van ruwe data, zodra de eerste publicatie daar is. Die data kunnen uit allerlei bronnen afkomstig zijn: EPD's, het laboratorium, imaging, uit sociale media, apps of andere ICT-applicaties, maar ook uit geheel andere bronnen buiten instituut, kliniek of laboratorium. Om databestanden bruikbaar en effectief te kunnen laten zijn, moet worden voldaan aan kwaliteitseisen. Die eisen zijn gegeven door het FAIR-concept: findable, accessible, interoperable en resusable.[4] Om dit praktisch mogelijk te maken in de dagelijkse praktijk van instituten zijn in Nederland de relevante partijen, waaronder NFU, VSNU en DTL, verenigd in 'Health-RI', een integraal ICT-infrastructuurplan voor de komende jaren om bigdataresearch te kunnen faciliteren, dat onderdeel is van de Nationale Wetenschapsagenda. Heel concreet bevat Health RI activiteiten als het NFU Data4Lifesciences-project met daarin bijvoorbeeld HANDS, een internettool voor data stewardship.[5] Daarnaast wordt binnen Data4LifeSciences voorgesorteerd op het gebruik van big data. Dit is nodig om richting te geven aan personalized medicine. Hierbij wordt een infrastructuur ontwikkeld die het voor alle instituten mogelijk maakt biomedische data over de instellingen heen te delen en te gebruiken inclusief de bijbehorende rekenkracht en bio-informatica. Dit geldt niet alleen voor de data die voortkomen uit de verschillende elektronische patiëntendossiers (EPD's), maar ook voor data die in de gehele keten, mede door de patiënt zelf,

4 http://www.thelancet.com/series/research.
5 http://data4lifesciences.nl/hands/handbook-for-adequate-natural-data-stewardship.

geproduceerd worden.[6] In Health RI zijn ook de grote biobanken en cohorten opgenomen waaraan enorme databases gekoppeld zijn en die volgens het FAIR-principe beschikbaar gemaakt zijn of zullen worden.

4 Science in transition

Onderzoekers die volgens de open-scienceprincipes gaan werken moeten op een ander wijze dan voorheen beoordeeld worden op hun impact. Hier is een rol weggelegd voor het hoger management van academische onderzoeksinstituten zoals het college van bestuur van de universiteiten, decanen van faculteiten en besturen van UMC's. Academisch onderzoek heeft vele vormen van excellentie en impact. In de onderhavige context van bigdataresearch zijn dat de klassieke artikelen in tijdschriften die peer reviewed zijn en in toenemende mate open access. Omdat open-accesstijdschriften lagere impactfactoren hebben, dient het gebruik van impactfactoren te worden vermeden, iets dat reeds langere tijd en in het algemeen wordt bepleit.[7] Daarnaast is het van belang dat onderzoekers kunnen aantonen dat hun datasets door collega's waar dan ook ter wereld worden gebruikt. Hiertoe dienen persoonlijke identificatiecodes van onderzoekers gekoppeld te zijn aan die datasets. Een voorbeeld hiervan is de ORCHID: Open Researcher Contributor Identification Initiative.[8] Ook de tijd en energie die onderzoekers steken in het verbeteren van de kwaliteit van het onderzoek door de kwaliteit van de data, de opslag van de data en de kwaliteit van de gekoppelde klinische data en de kwaliteit en toegankelijkheid van de biomaterialen, inclusief beeldmateriaal moet in de beoordeling integraal worden meegenomen. Helaas worden deze zogenaamde 'academic duties' die voor big data science cruciaal zijn, meestal nog niet in het eindejaargesprek op waarde geschat.
Deze transitie zal versneld worden als de organisaties die onderzoek subsidiëren voorwaarden gaan stellen aan de kwaliteit van data en datamanagement en het gebruik van de FAIR-principes in de instituten en door de onderzoeksleiders (PI's) die met hun subsidies onderzoek uitvoeren. Nu al maken onder andere de EU, NIH, Welcome Trust en in ons land NWO en de gezondheidsfondsen deze beweging of zijn in voorbereiding om deze te maken. Wij anticiperen dat de evaluatie van onderzoek en onderzoekers in de komende jaren deze transitie zal doormaken en naar een integrale beoordeling van impact zal komen.[9]
Door op deze wijze het incentive- en rewardsysteem meer integraal te maken zullen onderzoekers gestimuleerd worden om te gaan investeren in de kwaliteit van onderzoek wat zal leiden tot het faciliteren en succesvol versnellen van de vertaling van onderzoeksresultaten naar de praktijk.

---

6 http://www.dtls.nl/fair-data/personal-health-train.
7 http://www.hefce.ac.uk/pubs/rereports/Year/2015/metrictide/Title,104463,en.html en http://www.ascb.org/dora/.
8 https://dx.doi.org/10.1038%2F462825a.
9 http://www.nature.com/news/fewer-numbers-better-science-1.20858.

Literatuur

Merton (1973)
R. Merton, *The sociology of Science, Theoretical and Emperical Investigations*, The University of Chicago Press, Chicago, 1973.

Miedema (2012)
F. Miedema, *Science 3.0*, Amsterdam: Amsterdam University Press, 2012.

Jasanoff (2016)
S. Jasanoff, *The Ethics of Invention*, Norton, New York, 2016.

Nowotny (2016)
H. Nowotny, *The Cunning of Uncertainty*, Cambridge UK: Polity Press, 2016.

Deel 4
Big data en wetenschappelijk onderzoek

Deel 4B
Big data, medisch-wetenschappelijk onderzoek en gegevensbescherming

Mr. M. Mostert*

* Menno Mostert is docent gezondheidsrecht en promovendus bij de afdeling Medical Humanities van het Julius Centrum, UMC Utrecht.

1 Inleiding

Wereldwijd groeien de investeringen gestaag om met behulp van big data kennis over menselijke gezondheid en ziekte te verbeteren.[1] Kenmerkend voor het gebruik van big data in medisch-wetenschappelijk onderzoek is het verzamelen, hergebruiken, koppelen en analyseren van diverse, grote en/of complexe gegevensbestanden. Deze ontwikkeling wordt ook wel data-intensief gezondheidsonderzoek genoemd.[2] Daarbij gaat het zowel om analyse met behulp van traditionele als innovatieve methoden van wetenschappelijk onderzoek.[3] Vanaf 25 mei 2018 is het gebruik van persoonsgegevens in dergelijk onderzoek in de Europese Unie (EU) onderworpen aan de voorschriften in de Algemene Verordening Gegevensbescherming (AVG).[4] Gezien de uitgebreide bescherming in de AVG en het feit dat de verordening rechtstreekse werking zal hebben in alle EU-lidstaten, is dit een zeer belangrijke ontwikkeling. Ondanks de rechtstreekse werking behoeft een belangrijk deel van de bepalingen in de AVG die betrekking hebben op wetenschappelijk onderzoek wel omzetting in het nationale recht. De uitvoering en omzetting van de AVG in Nederland zal plaatsvinden in de Uitvoeringswet AVG, waarvan recent een consultatieversie verscheen.[5] Met de inwerkingtreding van de Uitvoeringswet AVG zal de Wet bescherming persoonsgegevens (Wbp) worden ingetrokken.

Het belang van data-intensief gezondheidsonderzoek, althans het koppelen van gegevens, wordt expliciet erkend in de AVG. De EU-wetgever overweegt dat 'onderzoekers nieuwe en zeer waardevolle kennis verwerven over veel voorkomende medische aandoeningen (..)' door gegevens te koppelen. Daarom dient, nog steeds volgens de EU-wetgever, wetenschappelijk onderzoek in de EU gefaciliteerd te worden door te bepalen dat 'persoonsgegevens, met inachtneming van de passende voorwaarden en waarborgen die in (..) het recht zijn vastgesteld, met het oog op wetenschappelijk onderzoek mogen worden verwerkt.'[6] Ook wordt

---

1 Bijv. the All of Us Research Program: https://www.nih.gov/AllofUs-research-program/pmi-cohort-program-announces-new-name-all-us-research-program (d.d. 09-12-2016); en dichter bij huis: de toekenning van € 20 miljoen aan het BigData@Heart-onderzoek: http://www.umcutrecht.nl/nl/Over-Ons/Nieuws/2016/%E2%82%AC20-miljoen-voor-UMC-Utrecht-voor-big-data-onderzo (09-12-2016).

2 M. Mostert, A.L. Bredenoord, M.C.I.H. Biesaart, J.J.M. van Delden, 'Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach', *European Journal of Human Genetics*, 2016;24:956-60.

3 Het gaat dus niet (alleen) om bigdataonderzoek zoals gedefinieerd in: L. Ottes, 'Big Data in de zorg', Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid, 2016, Working Paper 19.

4 Verordening (EU) 2016/679, PbEU 2016, L 119 http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&rid=1.

5 https://www.internetconsultatie.nl/uitvoeringswetavg (d.d. 24-12-2016).

6 Overweging 157 van de AVG.

verwezen naar de doelstelling van de EU om te komen tot een 'Europese onderzoeksruimte' zoals bedoeld in artikel 179 lid 1 van het Verdrag betreffende de Werking van de Europese Unie (VWEU).[7] Ondanks deze intenties werd, nadat het Europees Parlement voor een conceptversie van de AVG stemde, gevreesd dat de AVG medisch-wetenschappelijk onderzoek ernstig zou belemmeren.[8] Op de gewijzigde definitieve versie van de AVG werd daarentegen overwegend positief gereageerd. Al snel verscheen een ingezonden bericht in *The Lancet* inhoudende dat de AVG een stap voorwaarts betekent, zowel voor de bescherming van persoonsgegevens als het gebruik daarvan in biomedisch onderzoek.[9]
Uit een kort daarop volgende beknopte artikelsgewijze analyse in opdracht van The Wellcome Trust bleek echter dat de impact van de AVG op onderzoek in belangrijke mate afhangt van de interpretatie en omzetting van de AVG in de diverse lidstaten.[10] Daarbij bestaat onder meer onduidelijkheid over de definitie van persoonsgegevens, de voorwaarden voor een rechtsgeldige toestemming, de uitzonderingen op het toestemmingsvereiste, de afwijkingen van diverse beginselen en rechten en de bij uitzonderingen of afwijkingen vereiste passende waarborgen. In deze bijdrage vindt daarom een nadere analyse en beschouwing plaats met een focus op de bepalingen die specifiek zien op wetenschappelijk onderzoek. Hierin staat de vraag centraal of de AVG in positieve zin bijdraagt aan een verantwoord en effectief gebruik van persoonsgegevens in data-intensief gezondheidsonderzoek. Daarbij wordt ook aandacht besteed aan de consultatieversie van de Uitvoeringswet AVG.

2 Van privacy naar gegevensbescherming

Hoewel de EU-wetgever de verwerking van persoonsgegevens voor *onderzoeksdoeleinden* wenst te faciliteren,[11] stelt zij voorop dat dit dan wel dient te gebeuren met inachtneming van *passende waarborgen*. In de kern dienen deze waarborgen ertoe om fundamentele rechten van natuurlijke personen op passende wijze te beschermen. Opvallend is dat juist op het niveau van fundamentele rechten een verandering zichtbaar is in de AVG. Terwijl Richtlijn 95/46/EG in het bijzonder

7 Overweging 159 van de AVG.
8 Bijv. M.C. Ploem, M.L. Essink-Bot, K. Stronks, 'Proposed EU data protection regulation is a threat to medical research', *British Medical Journal*, 2013;346: f3534.
9 E.S. Dove, B. Thompson, B.M. Knoppers, 'A step forward for data protection and biomedical research', *The Lancet*, 2016;387:1374–5.
10 The Wellcome Trust, 'Analysis: Research and the General Data Protection Regulation', 2016, https://wellcome.ac.uk/sites/default/files/new-data-protection-regulation-key-clauses-wellcome-jul16.pdf (d.d. 09-01-2016).
11 Met de term 'onderzoeksdoeleinden' wordt in dit deel van het preadvies aangesloten bij de definitie van wetenschappelijk onderzoek in overweging 159 van de AVG.

het recht op privacy waarborgde,[12] waarborgt de AVG vooral het recht op gegevensbescherming. Dit blijkt onder meer uit artikel 1 lid 2 AVG, waarin als doelstelling is opgenomen dat de verordening de fundamentele rechten van natuurlijke personen beschermt 'en met name hun recht op bescherming van persoonsgegevens'. Daarnaast is het opvallend dat het gebruik van de term 'privacy' nagenoeg verdwenen is uit de (Engelse versie van) de AVG. Gebruikelijke termen als '*privacy by design*' en '*privacy impact assessment*' zijn gewijzigd in '*data protection by design*' en '*data protection impact assessment*'. Ook hiermee lijkt de EU-wetgever tot uitdrukking te brengen dat de bescherming van persoonsgegevens niet langer primair het recht op privacy waarborgt.
Deze wijzigingen in de AVG volgen op de erkenning van het recht op gegevensbescherming als een fundamenteel recht in de EU, afzonderlijk van en in aanvulling op het recht op privacy. De erkenning van het recht op gegevensbescherming ligt vast in artikel 8 van het Handvest van de Grondrechten van de EU (EU Handvest), terwijl de erkenning van het recht op privacy in artikel 7 EU Handvest vastligt. Het EU Handvest is sinds 2009 juridisch bindend voor de EU en voor haar lidstaten in situaties waarin deze EU-recht 'ten uitvoer brengen'.[13] Het EU Handvest is dus bij uitstek van toepassing bij de interpretatie en uitvoering van de AVG. Daarbij gaat het EU Handvest voor op het nationale recht en dus ook op artikel 10 van de Grondwet.[14] In dit beperkte toepassingsgebied verschilt het EU Handvest van het Europees Verdrag voor de Rechten van de Mens (EVRM), dat een uitgebreidere werking kent in de nationale rechtsorde. Ondanks deze beperking biedt het recht op gegevensbescherming in artikel 8 EU Handvest deels een verdergaand beschermingsniveau dan het recht op privacy zoals erkend in artikel 8 EVRM en artikel 7 EU Handvest.[15] Volgens de Interdepartementale Commissie Europees Recht (ICER) bestaat deze uitbreiding van het beschermingsniveau uit het erkennen van een recht op onafhankelijk toezicht in artikel 8 lid 3 EU Handvest.[16] Hier kan onder meer aan toegevoegd worden dat het waarborgen van het recht op gegevensbescherming voor de EU en haar lidstaten in de kern een positieve verplichting is om de verwerking van persoonsgegevens aan pas-

12 Art. 1 lid 1 Richtlijn 95/46/EG.
13 Zie uitvoerig: ICER handleiding nationale toepassing EU-Grondrechtenhandvest: http://www.minbuza.nl/binaries/content/assets/ecer/ecer/import/icer/handleidingen/2014/icer-handleiding-nationale-toetsing-eu-handvest-grondrechten.pdf (d.d. 09-12-2016).
14 Zie ook: consultatieversie Uitvoeringswet AVG, p. 21-23.
15 Zie over het recht op privacy in art. 8 EVRM, art. 17 IVBPR en art. 10 Grondwet: M.C. Ploem, *Tussen privacy en wetenschapsvrijheid, Regulering van gegevensverwerking voor medisch-wetenschappelijk onderzoek*, Den Haag: Sdu Uitgevers, 2004, p. 31-37.
16 ICER handleiding nationale toepassing EU-Grondrechtenhandvest, p. 9.

sende voorschriften te onderwerpen.[17] Dit geldt zowel voor de gegevensverwerking in horizontale relaties als voor die door publieke autoriteiten in verhouding tot de burger. Het recht op privacy is anders van karakter. Het respecteren van het recht op privacy houdt in de kern nog steeds een negatieve verplichting voor publieke autoriteiten in.[18] Hierbij past wel de nuancering dat artikel 8 EVRM in toenemende mate een positieve verplichting inhoudt om respect voor het recht op privacy te garanderen, ook tussen burgers onderling.[19] Desalniettemin mag op basis van het fundamentele recht op gegevensbescherming een actievere rol van de EU en haar lidstaten worden verwacht, om het verkeer van persoonsgegevens te beschermen conform de eisen die artikel 8 EU Handvest stelt. Het motief voor deze bescherming omvat ook de bevordering van collectieve belangen,[20] zoals het op verantwoorde wijze mogelijk maken van gegevensuitwisseling voor wetenschappelijke onderzoeksdoeleinden.

De EU-wetgever benadrukt dat deze belangen bij de bescherming van persoonsgegevens toenemen, gezien de snelle technologische en maatschappelijke veranderingen.[21] Dergelijke veranderingen zijn zeker ook aan de orde voor wat betreft de verwerking van gezondheidsgegevens en andere bijzondere persoonsgegevens. De tijd is voorbij waarin vooral hulpverleners over gezondheidsgegevens beschikten, die zij in het medisch dossier vastlegden. In toenemende mate worden gegevens over de gezondheid, de genen en leefstijl van personen ook buiten de hulpverlener om op grote schaal vastgelegd, gedeeld en/of hergebruikt, zonder dat deze gegevens onder de reikwijdte van het beroepsgeheim vallen. Voorbeelden van ontwikkelingen die hier, specifiek gericht op wetenschappelijk onderzoek, aan bijdragen zijn de opkomst van *citizen science* en *participant-driven research*,[22] maar zeker ook applicaties zoals ResearchKit van Apple waar wetenschappers op steeds grotere schaal gebruik van maken.[23] Daarnaast zal het recht van patiënten om een digitaal afschrift van het medisch dossier te ontvangen mogelijk bijdragen aan een verspreiding van patiëntgegevens buiten de hulpverlener om.[24] Ook

17 Dit blijkt o.m. uit de formulering van art. 8 lid 1 EU Handvest, 'een ieder heeft recht op bescherming [onderstreping: MM] van (..)'.

18 EHRM 16 juli 2014, ECLI:CE:ECHR:2014:0716JUD003735909 (*Hämäläinen t. Finland*).

19 Zie bijv.: EHRM, 26 maart 1985, *NJ* 1985, 525, m.nt. Alkema (*X en Y t. Nederland*).

20 E.M.L. Moerel, J.E.J. Prins, Privacy voor de homo digitalis, in: *Preadviezen NJV 2016-1*, Wolters Kluwer, 2016, p. 57-58.

21 Overweging 6 van de AVG.

22 Nuffield Council on Bioethics, 'The collection, linking and use of data in biomedical research and healthcare: ethical issues', 2015, p. 146-149, http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf (d.d. 24-12-2016).

23 Apple's ResearchKit frees medical research, *Nature Biotechnology*, 2015;33:322.

24 Zie: art. 15d lid 1 Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) voor het toekomstige recht op elektronische inzage en afschrift van het medisch dossier.

dit heeft tot gevolg dat het belang bij het overkoepelende regime van gegevensbescherming, naast de bescherming middels het beroepsgeheim,[25] toeneemt.

3 Herleidbaarheid in het tijdperk van big data

Het rechtmatige gebruik van persoonsgegevens voor onderzoeksdoeleinden wordt in de praktijk regelmatig mogelijk gemaakt door gegevens te anonimiseren. Ook komt het voor dat persoonsgegevens onterecht als anoniem worden beschouwd.[26] Dit is aantrekkelijk omdat het wettelijk regime van gegevensbescherming alleen van toepassing is op de verwerking van persoonsgegevens. Persoonsgegevens zijn gegevens die direct of indirect herleidbaar zijn tot een natuurlijk persoon (artikel 4 lid 1 AVG).[27] In artikel 89 lid 1 AVG wordt het gebruik van anonieme gegevens zelfs voorgeschreven, als de onderzoeksdoeleinden op die manier kunnen worden verwezenlijkt. Hoewel anonimisering op het eerste gezicht een bruikbare strategie voor wetenschappers lijkt om aan wettelijke vereisten te voldoen, is een kritische reflectie op de effectiviteit van anonimiseringstechnieken op zijn plaats. Dit geldt temeer nu de mogelijkheden tot profiling en re-identificatie toenemen met de opkomst van big data.

3.1 Het einde van anonimiteit?

Duidelijk is dat absolute anonimiteit niet langer te garanderen valt,[28] zeker wanneer het gaat om genetische gegevens.[29] Absolute anonimiteit is echter niet vereist op grond van het recht. Volgens overweging 26 van de AVG bepaalt een op redelijkheid gebaseerde toets of gegevens anoniem zijn:

---

25 Zie uitvoerig over de regeling van het beroepsgeheim in art. 7:457 en 7:458 BW: M.C. Ploem, 'Gegeven voor de wetenschap, Regulering van onderzoek met gegevens, lichaamsmateriaal en biobanken', in: *Wetenschappelijk onderzoek in de zorg*, Preadvies 2010 Vereniging voor Gezondheidsrecht, Den Haag: Sdu Uitgevers, 2010; Ploem, 2004.

26 Zie bijv. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_nza-dis.pdf (d.d. 24-12-2016).

27 In tegenstelling tot het beroepsgeheim (dat na overlijden doorwerkt) geldt de bescherming van persoonsgegevens op grond van de AVG alleen voor levende natuurlijke personen. Zie over lacunes in bescherming na overlijden: M.C. Ploem en J.C.J. Dute, Wetenschappelijk onderzoek na overlijden: goed geregeld?, *TvGR*, 2016;8:498-512.

28 Ottes, 2016.

29 N. Savage, 'The Myth of Anonimity', *Nature*, 2016;537:70-2; L.L. Rodriguez et al., 'Research ethics. The complexities of genomic identifiability', *Science* 2013; 339:275-6; M. Gymrek et al., 'Identifying personal genomes by surname inference', *Science* 2013;339:321-4.

> 'Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken.'

Gegevens zijn dus anoniem zodra directe of indirecte identificatie voorkomen wordt, uitgaande van de middelen die personen *redelijkerwijs* kunnen inzetten.
Bij de invulling van deze norm moet volgens voornoemde overweging van de AVG niet alleen rekening worden gehouden met de huidige technologie, maar ook met 'de technologische ontwikkelingen'. Technologische ontwikkelingen lijken vooralsnog vooral bij te dragen aan een verhoogde kans op re-identificatie. Uit advies 5/2014 van de Artikel 29-werkgroep bleek bijvoorbeeld dat geen van de geanalyseerde anonimiseringstechnieken met zekerheid voldeed aan de criteria voor een doeltreffende anonimisering.[30] Hierbij spelen volgens de Artikel 29-werkgroep niet alleen technische factoren een rol. Ook relevante contextuele factoren moeten in overweging worden genomen. Hierbij kan bijvoorbeeld gedacht worden aan maatregelen die de toegang tot de gegevens beperken, maar ook aan de beschikbaarheid van openbare informatiebronnen. Daarbij moet in aanmerking worden genomen dat de hoeveelheid informatie die openbaar beschikbaar is, of anderszins met een redelijke inspanning beschikbaar komt, exponentieel groeit. Daarnaast nemen ook de mogelijkheden van analyse toe, waardoor een combinatie van beschikbare bronnen al snel tot identificatie kan leiden.[31]
In een recent arrest van het Hof van Justitie van de EU (HvJ EU) wordt nader toegelicht wanneer extern beschikbare informatie moet worden beschouwd als een middel dat redelijkerwijs kan worden ingezet ter identificatie.[32] Volgens het Hof is dit niet het geval indien identificatie met behulp van deze extra informatie in de praktijk 'ondoenlijk is' althans 'het gevaar van identificatie in werkelijkheid onbeduidend lijkt'. Dit is bijvoorbeeld het geval als identificatie '(..) – gelet op de vereiste tijd, kosten en mankracht – een excessieve inspanning vergt'. Daarnaast overweegt het Hof dat ook een wettelijk verbod – dat toegang tot de extra informatie juridisch gezien onmogelijk maakt – ertoe kan leiden dat de extra informatie niet langer als een middel moet worden beschouwd dat redelijkerwijs ingezet kan worden ter identificatie van een persoon.
Hoewel het voldoen aan voornoemde juridische maatstaf van anonimiteit niet onmogelijk is, heeft een doeltreffende anonimisering wel tot gevolg dat de bruikbaarheid van de gegevens voor onderzoeksdoeleinden aanzienlijk afneemt. Ten

30 Zie http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (09-12-2016).
31 S. Barocas, H. Nissenbaum, 'Big data's end run around anonymity and consent', in: J. Lane et al. (eds.), *Privacy, big data, and the public good: Frameworks for Engagement*, Cambridge: Cambridge University Press, 2014, p. 44-75.
32 HvJEU 19 oktober 2016, ECLI:EU:C:2016:779 (*Breyer*).

eerste wordt dit veroorzaakt doordat veel van de bruikbare gegevens uit een bestand verwijderd moeten worden om herleiding tot het individu redelijkerwijs te voorkomen. Ten tweede lijkt anonimisering te voorkomen dat gegevensbestanden nog gekoppeld of geactualiseerd kunnen worden. Dit zou data-intensief gezondheidsonderzoek ernstig belemmeren, omdat de mogelijkheid tot koppeling en actualisering van gegevens een van de kernelementen van dergelijk onderzoek betreft.[33]

3.2 Pseudonimiseren ter vermindering van risico's

Hoewel het gros van de nadelen van het gebruik van anonieme gegevens ook geldt voor de inzet van pseudonieme gegevens,[34] blijven de mogelijkheden tot koppeling en actualisering van gegevens na pseudonimisatie wel deels bestaan.[35] Van Veen stelde mede daarom voor om pseudonieme (dubbel gecodeerde) gegevens die voor onderzoeksdoeleinden worden gebruikt als anoniem te beschouwen.[36] In de AVG wordt echter benadrukt dat pseudonimisering weliswaar een middel is om risico's te verminderen, maar dat het niet bedoeld is om andere gegevensbeschermingsmaatregelen uit te sluiten.[37] De EU-wetgever lijkt hiermee op ondubbelzinnige wijze te bevestigen dat pseudonieme gegevens als persoonsgegevens moeten worden beschouwd.
Voornoemde uitspraak van het HvJ EU biedt echter ruimte voor enige twijfel hierover, indien en voor zover een verbod tot indirecte identificatie wettelijk ingevoerd zou worden. Het moet dan gaan om een verbod dat toegang tot de extra informatie – die nodig is om de pseudonieme gegevens te herleiden tot het individu – juridisch gezien absoluut onmogelijk maakt.[38]

---

33 P. Quinn, 'The Anonymisation of Research Data — A Pyric Victory for Privacy that Should Not Be Pushed Too Hard by the EU Data Protection Framework?', *European Journal of Health Law*, 2016;24:1-24; O.Tene, J. Polonetsky: 'Privacy in the age of Big Data: a time for big decisions,' *Stanford Law Rev Online* 2012;64:63–9; B.M. Knoppers, M.H. Zawati, E.S. Kirby, 'Sampling populations of humans across the world: ELSI issues', *Annu Rev Genomics Hum Genet* 2012;13:395-413; Mostert et al, 2016.

34 Zie art. 4 lid 5 AVG voor de definitie van pseudonimisering.

35 Nuffield Council on Bioethics, 2015, p. 68-73.

36 E.B. van Veen, 'Europe and tissue research: a regulatory patchwork', *Diagn Histopathol*, 2013;19:331–6. Zie ook: W.W. Lowrance, 'Privacy, Confidentiality, and Health Research', Cambridge University Press: Cambridge, UK, 2012, p. 158.

37 Overweging 28 van de AVG.

38 HvJEU 19 oktober 2016, ECLI:EU:C:2016:779 (*Breyer*).

3.3 Status lichaamsmateriaal

Genetische gegevens vallen onder de bescherming van de AVG als voldaan is aan de definitie in artikel 4 lid 13 AVG. Uit dit artikellid valt af te leiden dat het lichaamsmateriaal zelf niet onder de definitie van genetische gegevens valt. Het gaat volgens deze definitie immers (met name) om gegevens die 'voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon.' Overweging 34 van de AVG bevestigt dat het gaat om gegevens 'die blijken uit een analyse van een biologisch monster'. In de memorie van toelichting (MvT) bij de consultatieversie van de Uitvoeringswet AVG is echter de volgende afwijkende definitie opgenomen: 'Hieronder wordt onder andere verstaan het DNA van een persoon of materiaal waaruit informatie met betrekking tot het DNA kan worden afgeleid'. Volgens deze omschrijving valt ook het lichaamsmateriaal zelf, waaruit informatie met betrekking tot het DNA kan worden afgeleid, onder de definitie van genetische gegevens.
Daarentegen moet de opslag van lichaamsmateriaal *op zichzelf* wel als een inbreuk op het recht op privacy worden beschouwd. Dit blijkt uit de volgende overweging van het Europees Hof voor de Rechten van de Mens (EHRM) in de zaak *S. en Marper t. Verenigd Koninkrijk*:

> 'Given the nature and the amount of personal information contained in cellular samples, their retention per se must be regarded as interfering with the right to respect for the private lives of the individuals concerned.'[39]

Het EHRM concludeert daarnaast dat de opslag van lichaamsmateriaal in het bijzonder inbreuk maakt op het recht op privacy, 'given the wealth of genetic and health information contained therein.'[40] Ploem sluit zich aan bij deze conclusie, omdat de (toekomstige) potentie om gevoelige informatie af te leiden volgens haar groter is bij lichaamsmateriaal dan bij een combinatie van gegevensbestanden.[41]

3.4 Deelconclusie

Uit het voorgaande blijkt dat het gebruik van anonimiseringstechnieken vaak een onvoldoende betrouwbare strategie is om de belangen en rechten van betrokkenen te beschermen. Ook als gegevens eenmaal als anoniem zijn bestempeld, blijft overigens de noodzaak bestaan om deze anonimiteit te monitoren en controle te houden over de context waarin de gegevens zich bevinden. Daarnaast zijn daadwerkelijk anonieme gegevensbestanden nagenoeg onbruikbaar voor de doeleinden gerelateerd aan data-intensief gezondheidsonderzoek. Iedere claim inhou-

39 EHRM 04-12-2008, ECLI:NL:XX:2008:BH1813, § 72.
40 EHRM 04-12-2008, ECLI:NL:XX:2008:BH1813, § 120.
41 Ploem, 2010, p. 153-156.

dende dat voor gezondheidsonderzoek bruikbare gegevensbestanden anoniem zijn, dient daarom kritisch onder de loep te worden genomen, zeker als het gaat om genetische gegevens of openbaar beschikbare gegevensbestanden.
Hoewel de opslag van lichaamsmateriaal als een inbreuk op het recht op privacy moet worden beschouwd, lijkt lichaamsmateriaal op zichzelf niet onder de definitie van persoonsgegevens of genetische gegevens in de AVG te vallen. Mijns inziens dient de afwijkende definitie in de consultatieversie van de Uitvoeringswet AVG dan ook aangepast te worden of van een nadere toelichting te worden voorzien. Mocht de Nederlandse wetgever vasthouden aan voornoemde definitie, dan is het wel van belang dat een onderscheid aangebracht wordt tussen het lichaamsmateriaal dat wel en het lichaamsmateriaal dat niet als persoonsgegevens moet worden beschouwd. Dit onderscheid zou dan gekoppeld kunnen worden aan het doel van de opslag van het lichaamsmateriaal. Zodra het doel van de opslag is om informatie uit het lichaamsmateriaal af te leiden en het redelijkerwijs mogelijk is om deze informatie tot het individu te herleiden, kan overwogen worden om het lichaamsmateriaal als persoonsgegeven aan te merken. Gezien het toenemende potentieel om bijzondere persoonsgegevens af te leiden uit lichaamsmateriaal, zou dit de bescherming van het individu ten goede komen. Op basis van de definities in de AVG concludeer ik echter dat niet eerder persoonsgegevens verwerkt worden dan op het moment dat deze door middel van een analyse afgeleid worden uit het lichaamsmateriaal. De noodzaak van specifieke wetgeving voor het gebruik van lichaamsmateriaal blijft dus bestaan, ook vanwege de bijzondere aard en gevoelige status van lichaamsmateriaal.

4 Toestemming: specifiek of ruim?

Wanneer anonimisering geen wenselijke strategie blijkt om gegevens te gebruiken in data-intensief gezondheidsonderzoek, is het vragen van toestemming aan de betrokkene een mogelijkheid om persoonsgegevens op rechtmatige wijze te verwerken in data-intensief gezondheidsonderzoek.[42] Een breed gedeelde opvatting in de literatuur is echter dat streng vasthouden aan het toestemmingsvereiste een effectieve inzet van persoonsgegevens in data-intensief gezondheidsonderzoek belemmert of zelfs onmogelijk maakt.[43] De onmogelijkheden of belemmerende factoren gelden vooral als de toestemming beperkt is tot zeer specifieke doeleinden, waardoor in het geval van hergebruik of koppeling telkens opnieuw toestemming gevraagd moet worden. De uitwerking en interpretatie van het toestemmingsvereiste, en in het bijzonder de mate waarin de doeleinden van de verwerking gespecificeerd moeten worden, is daarom van groot belang.

42 Zie par. 5 voor de rechtmatigheid van verwerking van persoonsgegevens voor onderzoeksdoeleinden zonder toestemming.
43 Zie: Mostert et al., 2016.

4.1 Ontvlechten van toestemmingsvereisten

Over het algemeen zal in data-intensief gezondheidsonderzoek moeten worden voldaan aan het specifieke regime in artikel 9 AVG, omdat aangenomen mag worden dat in dergelijk onderzoek zelden géén bijzondere (categorieën van) persoonsgegevens, zoals gegevens over de gezondheid, worden verwerkt.[44] Bijzondere persoonsgegevens mogen niet worden verwerkt behoudens de uitdrukkelijk in artikel 9 AVG genoemde gevallen, waaronder de uitdrukkelijke toestemming van de betrokkene conform artikel 9 lid 2 sub a AVG. Het verbod en de specifieke voorschriften in artikel 9 AVG zijn een aanvulling op de algemene beginselen en regels van de AVG. Uitzonderingen op het verbod van artikel 9 AVG zijn alleen toegestaan onder de specifieke voorwaarden waarin uitdrukkelijk wordt voorzien.[45] Het vereiste van uitdrukkelijke toestemming in artikel 9 lid 2 sub a AVG is een bijzondere bepaling, die in aanvulling geldt en voorrang heeft ten opzichte van het algemene toestemmingsvereiste. Het is daarom van belang om een onderscheid te maken tussen deze twee verschillende toestemmingsvereisten.

4.1.1 Het algemene toestemmingsvereiste

Het algemene toestemmingsvereiste is in artikel 4 lid 11 AVG gedefinieerd als een 'vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting' waarmee de betrokkene de verwerking aanvaardt. De toestemming moet op grond van artikel 6 lid 1 sub a AVG voor 'een of meer specifieke doeleinden' gegeven worden. Zoals hiervoor reeds toegelicht, heeft onverkort vasthouden aan dit laatstgenoemde vereiste van doelbinding een sterk belemmerend effect op data-intensief gezondheidsonderzoek. De EU-wetgever overweegt dan ook dat het, op het ogenblik dat de persoonsgegevens worden verzameld, vaak niet mogelijk is om het doel van de gegevensverwerking volledig te omschrijven. Hij overweegt daarop het volgende:

> 'Daarom moet de betrokkenen worden toegestaan hun toestemming te geven voor bepaalde terreinen van het wetenschappelijk onderzoek waarbij erkende ethische normen voor wetenschappelijk onderzoek in acht worden genomen.'[46]

De toestemming voor bepaalde onderzoeksterreinen zoals hier omschreven toont sterke gelijkenissen met wat ook wel 'broad consent' wordt genoemd. Overweging 33 van de AVG vormt dan ook een aanknopingspunt voor nationale wetgevers en

---

44 Voor kritiek op het onderscheid in bescherming tussen persoonsgegevens en bijzondere persoonsgegevens: Moerel en Prins, 2016, p. 82-90.

45 Overweging 51 van de AVG.

46 Overweging 33 van de AVG.

beleidsmakers om broad consent als een rechtmatige vorm van toestemming te beschouwen in de zin van artikel 6 lid 1 sub a AVG.
Daarbij overweegt de EU-wetgever wel uitdrukkelijk dat dan erkende ethische normen voor wetenschappelijk onderzoek in acht moeten worden genomen. Een recent document waarin dergelijke ethische normen zijn vastgelegd is de World Medical Association Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks (WMA Declaration of Taipei).[47] Volgens de WMA Declaration of Taipei is broad consent alleen geldig indien het individu is geïnformeerd over de in paragraaf 12 genoemde onderwerpen, waaronder de *governance*-maatregelen genoemd in paragraaf 21.[48] Daarbij moet wel opgemerkt worden dat de Declaration of Taipei zich primair richt tot artsen. De tevens recente Council for International Organizations of Medical Sciences International Ethical Guidelines for Health-related Research Involving Humans (CIOMS Guidelines) richten zich tot een breder publiek.[49] Guideline 12 van de CIOMS Guidelines bevestigt dat broad consent een acceptabel alternatief is, zolang dit samengaat met een passende governance van de gegevensverzameling.[50] Benadrukt wordt dat broad consent in essentie toestemming op basis van (informatie over) een adequaat governancesysteem is.[51]

4.1.2 Toestemmingsvereiste voor verwerking bijzondere persoonsgegevens

Zodra bijzondere persoonsgegevens worden verwerkt voor onderzoeksdoeleinden, gelden de voorschriften in artikel 9 lid 2 sub a AVG in aanvulling op of in afwijking van het algemene toestemmingsvereiste. Dit artikellid eist dat de toestemming 'uitdrukkelijk' is en gegeven voor 'een of meer welbepaalde doeleinden'. De term welbepaald is enigszins ongelukkig gekozen.[52] De Engelstalige versie van de AVG biedt een taalkundige opheldering, waarin de term '*specified purposes*' wordt gebezigd. De uitdrukkelijke toestemming op grond van artikel 9 lid 2 sub a AVG moet dus betrekking hebben op de verwerking voor gespecificeerde of precies omschreven doeleinden.

---

47 WMA Declaration of Taipei, 2016, http://www.wma.net/en/30publications/10policies/d1/ (d.d. 09-12-2016).

48 Onder *governance*(maatregelen) worden hier en elders in dit deel van het preadvies de organisatorische en technische maatregelen verstaan die genomen worden op het niveau van (een groep van) instellingen en/of ondernemingen.

49 CIOMS Guidelines, 2016, http://www.cioms.ch/ethical-guidelines-2016/ (d.d. 09-12-2016).

50 Zie par. 5.3 van dit deel van het preadvies over de governancemaatregelen vereist op grond van de CIOMS Guidelines en de WMA Declaration of Taipei.

51 J.J.M. van Delden, R. van der Graaf, 'Revised CIOMS International Ethical Guidelines for Health-Related Research Involving Humans', *JAMA*. Published online December 06, 2016. doi:10.1001/jama.2016.18977.

52 Ook een breed omschreven doel kan immers welbepaald zijn.

De kernvraag is vervolgens of broad consent (toestemming voor bepaalde onderzoeksterreinen) ook voldoet aan het vereiste van toestemming zoals omschreven in artikel 9 lid 2 sub a AVG. De specifieke voorschriften zoals opgenomen in artikel 9 AVG en de aan dit artikel gerelateerde overwegingen voorzien niet in een afwijking op het vereiste van specificiteit of doelbinding. Daarnaast is overweging 33 van de AVG niet uitdrukkelijk gericht op de verwerking van bijzondere persoonsgegevens; verwijzingen naar artikel 9 AVG of het specifieke regime voor dergelijke gegevens ontbreken volledig. Hierbij moet bedacht worden dat afwijkingen van het verbod in artikel 9 AVG alleen zijn toegestaan voor zover daar uitdrukkelijk in is voorzien.[53] Uit de consultatieversie van de Uitvoeringswet AVG blijkt echter dat het ministerie van Veiligheid en Justitie aanneemt dat overweging 33 van de AVG wel degelijk ook betrekking heeft op het vereiste van uitdrukkelijke toestemming. Dit wordt ondubbelzinnig bevestigd in de MvT bij de consultatieversie.[54]

4.2 Deelconclusie

Hoewel de EU-wetgever een verruiming van het toestemmingsvereiste toelaat waar het gaat om de verwerking van persoonsgegevens voor onderzoeksdoeleinden, is het onduidelijk of deze verruiming ook onverkort geldt voor de verwerking van *bijzondere* persoonsgegevens. Artikel 9 AVG voorziet namelijk in een specifiek regime dat zelf niet uitdrukkelijk voorziet in een afwijking van het vereiste van specifieke toestemming. Indien dit zou betekenen dat broad consent niet toegestaan is voor de verwerking van bijzondere persoonsgegevens, beperkt dit aanzienlijk de mogelijkheden tot het verkrijgen van een rechtsgeldige toestemming in data-intensief gezondheidsonderzoek. Het is onduidelijk of dit de bedoeling is van de EU-wetgever. Voor de rechtszekerheid is het van belang dat de Europese Commissie of een andere autoriteit hierover meer helderheid biedt.
Indien aangenomen kan worden dat broad consent is toegestaan voor de verwerking van bijzondere persoonsgegevens voor onderzoeksdoeleinden, dan dient de verwerking minimaal aan de eisen in overweging 33 van de AVG te voldoen. Dit betekent dat broad consent gericht moet zijn op bepaalde terreinen van wetenschappelijk onderzoek en erkende ethische normen in acht moeten worden genomen. De rechtmatigheid van broad consent hangt daardoor mede af van het naleven van dergelijke erkende ethische normen. Hieruit volgt dat erkende ethische normen, zoals vastgelegd in de CIOMS Guidelines en de WMA Declaration of Taipei, een sterkere juridische betekenis krijgen.

53 Zie ook par. 4.1 van dit deel van het preadvies.
54 Consultatieversie Uitvoeringswet AVG, p. 57.

5 Alternatief voor het toestemmingsvereiste

Als alternatief voor het toestemmingsvereiste kan lidstatelijk of EU-recht voorzien in een bepaling die specifiek de verwerking van bijzondere persoonsgegevens voor onderzoeksdoeleinden uitzondert van het verbod in artikel 9 AVG.[55] Hoewel het belang bij een dergelijke uitzondering nauwelijks ter discussie staat, geldt dit wel voor de wenselijke invulling ervan vanuit juridisch en ethisch perspectief.[56] Tegen deze achtergrond wordt hieronder gereflecteerd op de voorwaarden die artikel 9 lid 2 sub j AVG verbindt aan het bieden van een alternatief voor het toestemmingsvereiste in het nationale recht. Daarbij komt tevens aan de orde hoe deze bepaling volgens de consultatieversie van de Uitvoeringswet AVG omgezet moet worden in Nederlands recht.

5.1 Noodzakelijkheid en evenredigheid

De gegevensverwerking moet op grond van artikel 9 lid 2 sub j AVG ten eerste noodzakelijk zijn en in een evenredige verhouding staan tot de onderzoeksdoeleinden. Daarmee benadrukt de AVG de belangrijke rol die de beginselen van noodzakelijkheid en evenredigheid spelen. Over de wenselijke invulling van deze fundamentele beginselen werd verschillend gedacht door het Europees Parlement en de Raad van Ministers. Het Europees Parlement stemde op 12 maart 2014 voor een conceptversie van de AVG waarin een uitzondering alleen is toegestaan voor onderzoek dat een *high public interest* dient.[57] Gevreesd werd dat dit vereiste gezondheidsonderzoek in ernstige mate zou belemmeren.[58] De Raad van Ministers bereikte vervolgens overeenstemming over een conceptversie van de AVG waarin aanzienlijk meer ruimte werd geboden voor een uitzonderingsbepaling.[59] Uiteindelijk is een compromis gesloten dat heeft geresulteerd in bovengenoemde open normen die een nadere invulling vergen.

---

55 Zie art. 9 lid 2 sub j AVG. Hoewel art. 9 lid 2 sub h en i AVG betrekking kunnen hebben op het grensvlak van wetenschappelijk onderzoek en kwaliteitsmanagement, sociale gezondheidszorg of monitoring van de volksgezondheid, komen deze uitzonderingen hierna niet aan de orde. Dit mede om dit deel van het preadvies af te bakenen ten opzichte van de bijdrage van mr. E.B. van Veen.

56 Mostert et al., 2016.

57 Europees Parlement, wetgevingsresolutie van 12 maart 2014 over het voorstel voor een algemene verordening gegevensbescherming, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN (d.d. 09-12-2016).

58 Ploem et al., 2013.

59 Raad van Ministers, goedkeuring op 11 juni 2015 van het voorstel voor een algemene verordening gegevensbescherming, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf (d.d. 09-12-2016).

Over de wenselijke nadere invulling van de reikwijdte van een alternatief voor het toestemmingsvereiste voor medisch-wetenschappelijk onderzoek bestaan uiteenlopende opvattingen in de literatuur.[60] Ook bestaan grote verschillen tussen de ethische normen zoals erkend in de CIOMS Guidelines en die in de WMA Declaration of Taipei. Volgens de WMA Declaration of Taipei is een uitzondering op het toestemmingsvereiste alleen toegestaan indien een ethische commissie vooraf goedkeuring verleent. Daarnaast kan deze ethische commissie het toestemmingsvereiste alleen terzijde schuiven in het geval van een concrete, serieuze en onmiddellijke bedreiging van de volksgezondheid.[61] De WMA lijkt met deze voorwaarde tot uitdrukking te brengen dat volgens haar het belang bij vooruitgang van de medische wetenschap op zichzelf nooit voldoende is om het toestemmingsvereiste terzijde te schuiven.
De CIOMS Guidelines zijn aanzienlijk minder strikt en noemen twee situaties waarin uitzonderingen op het toestemmingsvereiste mogelijk zijn.[62] Ten eerste gaat het om de situatie waarin gegevens gebruikt worden die reeds verzameld worden in de context van routinematige klinische zorg. Een geïnformeerde opt-outprocedure is dan voldoende volgens richtlijn 12. Deze opt-outprocedure dient te voldoen aan de volgende voorwaarden: a) patiënten moeten op de hoogte zijn van de procedure; b) aan patiënten moet voldoende informatie worden verstrekt; c) patiënten moeten gewezen worden op het recht om hun gegevens terug te trekken; en d) voor patiënten moet een reële mogelijkheid bestaan om bezwaar te maken. Daarbij moet opgemerkt worden dat het in de context van klinische zorg veelal om gegevens gaat die onder het beroepsgeheim vallen, waarop een strenger juridisch regime van toepassing is. Het uitgangspunt van een opt-outregime valt in Nederland moeilijk met het huidige regime in overeenstemming te brengen. Op grond van artikel 7:458 Burgerlijk Wetboek (BW) dient immers om toestemming te worden gevraagd, tenzij dit in redelijkheid niet mogelijk is of in redelijkheid niet kan worden verlangd.[63] Pas nadat aan een van deze voorwaarden is voldaan geldt een geen-bezwaarsysteem dat gelijkenissen vertoont met voornoemde opt-outprocedure. Ten tweede beschrijft richtlijn 12 van de CIOMS Guidelines de situatie waarin onderzoekers gegevens wensen te gebruiken die in het verleden verzameld zijn voor onderzoeksdoeleinden, zonder dat toestemming is gegeven voor toekomstig gebruik. In dat geval kan een ethische commissie afwijkingen van het toestemmingsvereiste goedkeuren, als voldaan is aan de volgende cumulatieve voorwaarden. Het onderzoek moet: a) niet haalbaar of uitvoerbaar zijn om toestemming te vragen; b) *important social value* hebben;[64] en

60 Mostert et al., 2016.
61 WMA Declaration of Taipei, par. 16.
62 CIOMS Guidelines, richtlijn 12.
63 Zie uitgebreider over art. 7:458 BW: Ploem, 2010; B. Sluyters en M.C.I.H. Biesaart, *De geneeskundige behandelingsovereenkomst na invoering van de WGBO*, Zwolle: W.E.J. Tjeenk Willink, 1995.
64 Zoals gedefinieerd in CIOMS Guidelines, richtlijn 1.

c) niet meer dan een minimaal risico opleveren voor de deelnemers of de groep waartoe zij behoren.[65]
De invulling van voornoemde beginselen in de consultatieversie van de Uitvoeringswet AVG is van gelijke strekking als in het huidige artikel 23 lid 2 Wbp.[66] De verwerking moet volgens artikel 27 van de consultatieversie van de Uitvoeringswet AVG 'noodzakelijk' zijn voor onderzoek dat 'een algemeen belang' dient. Aangezien wetenschappelijk onderzoek veelal een algemeen belang dient, zal dit vereiste geen noemenswaardige beperkingen opleveren. Wel dwingt het aan het noodzakelijkheidsvereiste gelieerde beginsel van subsidiariteit om na te gaan of het onderzoeksdoel niet op een andere wijze kan worden verwezenlijkt, die voor de betrokkenen minder ingrijpend is. Het verbod is volgens artikel 27 van de consultatieversie van de Uitvoeringswet AVG dan ook alleen niet van toepassing als het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning vergt. Of sprake is van een 'onevenredige inspanning' hangt volgens de MvT bij de Wbp mede af van de mate waarin wegen openstaan om de betrokkenen te informeren. Daarbij dient in aanmerking te worden genomen of een medium beschikbaar is waarvan mag worden aangenomen dat het de betrokkenen voor een groot deel bereikt.[67] Een voorbeeld van zo'n medium zijn de portalen of interfaces die digitale communicatie met grote groepen (potentiële) deelnemers mogelijk maken, waarvan *dynamic consent* een voorbeeld is.[68]

5.2 Eerbiediging recht op gegevensbescherming

Ten tweede dient op grond van artikel 9 lid 2 sub j AVG 'de wezenlijke inhoud van het recht op bescherming van persoonsgegevens' geëerbiedigd te worden.[69] Een concrete duiding van de wijze waarop aan deze voorwaarde voldaan wordt of moet worden, ontbreekt in de consultatieversie van de Uitvoeringswet AVG. Dit draagt niet bij aan rechtszekerheid hierover.
Hoewel het vaststellen van wat de wezenlijke inhoud of essentie van een fundamenteel recht behelst, in het algemeen geen simpele kwestie is, bevat de tekst van artikel 8 EU Handvest vrij concrete aanwijzingen. Tot de wezenlijke inhoud beho-

65 CIOMS Guidelines, richtlijn 12.
66 Consultatieversie Uitvoeringswet AVG, art. 27 en p. 81.
67 MvT, *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 126 en 155. Aangezien de regering benadrukt dat zij met de Uitvoeringswet AVG zo dicht mogelijk bij het bestaande nationale recht beoogt te blijven, blijft de MvT bij de Wbp van belang voor de interpretatie van de artikelen die van gelijke strekking blijven in de Uitvoeringswet AVG.
68 J. Kaye et al., 'Dynamic consent: a patient interface for twenty-first century research networks', *European Journal of Human Genetics*, 2014;23:141–146.
69 De Wellcome Trust benadrukte reeds de noodzaak van nadere uitleg door de Europese Commissie over hoe deze voorwaarde vervuld kan worden. Zie: Wellcome Trust, 2016.

ren op grond van artikel 8 lid 2 EU Handvest de beginselen van eerlijkheid of behoorlijkheid, doelbinding en rechtmatigheid. Verder dienen de rechten op toegang tot gegevens en rectificatie daarvan geëerbiedigd te worden. Daarnaast moet volgens artikel 8 lid 3 EU Handvest worden voorzien in onafhankelijk toezicht. Verder kunnen ook andere elementen tot de wezenlijke inhoud van het recht op gegevensbescherming gerekend worden op grond van artikel 8 lid 1 EU Handvest.
De specifieke voorschriften voor de verwerking van bijzondere persoonsgegevens lijken dus onder meer te eisen dat het beginsel van doelbinding in acht wordt genomen, als een uitzondering op grond van artikel 9 lid 2 sub j AVG wordt toegestaan. Het beginsel van doelbinding behoort immers tot de wezenlijke inhoud van het recht op gegevensbescherming. Het is echter onduidelijk hoe dit vereiste, dat voortkomt uit het specifieke regime van bescherming op grond van artikel 9 AVG, zich verhoudt tot de algemene regels die gelden voor de verwerking van persoonsgegevens. De algemene regels bepalen dat de verdere verwerking voor onderzoeksdoeleinden onder bepaalde voorwaarden niet gebonden is aan het beginsel van doelbinding (artikel 5 lid 1 sub b AVG). Deze uitzondering op het beginsel van doelbinding richt zich echter niet uitdrukkelijk op de verwerking van bijzondere persoonsgegevens. Zowel in artikel 5 AVG zelf als in de aan dit artikel gerelateerde overwegingen wordt niet gerefereerd aan het specifieke regime van bescherming conform artikel 9 AVG. Aangezien uitdrukkelijk in afwijkingen van het verbod van artikel 9 AVG dient te worden voorzien, is het onduidelijk of het beginsel van doelbinding (onverkort) in acht genomen dient te worden.

5.3 Waarborgen op grond van artikel 89 lid 1 AVG

Ten derde dient de uitzonderingsbepaling onderworpen te worden aan de passende waarborgen zoals omschreven in artikel 89 lid 1 AVG. De waarborgen moeten volgens de eerste zin van dit artikellid in overeenstemming zijn met de AVG en de rechten en vrijheden van de betrokkene. In de Nederlandse versie van de AVG luidt de tweede zin als volgt:

> 'Die waarborgen zorgen ervoor dat er technische en organisatorische maatregelen zijn getroffen om de inachtneming van het beginsel van minimale gegevensverwerking te garanderen.'

Op basis van deze tekst lijken de op grond van artikel 89 lid 1 AVG vereiste waarborgen zich te beperken tot governancemaatregelen die het beginsel van minimale gegevensverwerking garanderen. Deze maatregelen 'kunnen' pseudonimisering of anonimisering omvatten, zolang dit verwezenlijking van de onderzoeksdoeleinden niet in de weg staat. Het lijkt dus te gaan om een facultatief voorschrift waarvan al snel in het belang van de onderzoeksdoeleinden kan worden afgeweken. Daar komt bij dat de verwerking op grond van artikel 5 lid 1 sub c

AVG toch al moet voldoen aan het beginsel van minimale gegevensverwerking. Afgaande op de Nederlandse versie van de AVG, voegt artikel 89 lid 1 AVG daarom weinig toe aan het reeds geldende regime van gegevensbescherming. De tweede zin van artikel 89 lid 1 in de Engelse versie van de AVG luidt echter als volgt:

> 'Those safeguards shall ensure that technical and organisational measures are in place in particular [onderstreping: MM] in order to ensure respect for the principle of data minimisation.'

De governancemaatregelen kunnen dus weliswaar *met name* zien op het garanderen van het beginsel van dataminimalisatie, maar dienen zich daartoe niet te beperken.[70] Artikel 89 lid 1 AVG en de aan dat artikellid gerelateerde overwegingen bevatten geen concrete aanwijzingen over mogelijke andere governancemaatregelen.
Vanuit ethisch perspectief zijn de benodigde governancemaatregelen beter uitgekristalliseerd. De CIOMS Guidelines en WMA Declaration of Taipei bevatten relatief concrete en specifieke normen gericht op de totstandbrenging van een passende governancestructuur. Hoewel deze normen niet juridisch bindend zijn, beogen ze wel bij te dragen aan wet- en regelgeving op dit vlak.[71] De CIOMS Guidelines en de WMA Declaration of Taipei vullen de juridische normen in de AVG onder meer aan door te bepalen dat in de governancestructuur voorzien moet zijn in: mechanismen rond het opnieuw contact opnemen met het individu; het onthullen van toevalsbevindingen en het communiceren van wetenschappelijke bevindingen; een orgaan dat uitgiftes van gegevens voor onderzoek beoordeelt en de voorwaarden waaronder dit gebeurt; en participatie door patiëntgroepen of de bredere gemeenschap.[72]
Artikel 89 lid 1 AVG heeft rechtstreekse werking in de Nederlandse rechtsorde en vergt geen omzetting in nationaal recht. Aan de voorwaarden van artikel 89 lid 1 AVG dient dan ook te worden voldaan, naast aan die in artikel 27 van de consultatieversie Uitvoeringswet AVG. Het verdient aanbeveling om dit expliciet tot uitdrukking te brengen in de toelichting bij de Uitvoeringswet AVG.

5.4 Aanvullende specifieke maatregelen

Ten vierde dienen passende en specifieke maatregelen ter bescherming van de grondrechten en belangen van de betrokkene te worden getroffen, naast de maatregelen die reeds vereist zijn op grond van artikel 89 lid 1 AVG. Artikel 9 lid 2 sub j AVG benadrukt hiermee dat alleen maatregelen op grond van artikel 89 lid 1

70 Zie voor een juiste weergave in het Nederlands ook overweging 156 van de AVG, tweede zin.
71 Zie bijvoorbeeld: WMA Declaration of Taipei, par. 24.
72 Zie het commentaar op CIOMS Guidelines, richtlijn 12 en WMA Declaration of Taipei, par. 20 en 21.

AVG niet volstaan. Passende maatregelen moeten worden getroffen, specifiek gericht op een alternatief voor het toestemmingsvereiste. De AVG bevat echter geen aanwijzingen waaruit blijkt om wat voor passende en specifieke maatregelen het zou moeten gaan, of op welke wijze gegarandeerd moet worden dat deze maatregelen worden getroffen. Een nadere invulling hiervan kan nog plaatsvinden in EU- of nationaal recht.
De consultatieversie van de Uitvoeringswet AVG concretiseert niet welke aanvullende specifieke maatregelen dienen te worden getroffen. Deze voorwaarde lijkt op te gaan in het algemene vereiste in artikel 27 sub c van de consultatieversie.

5.5 Verwerking genetische gegevens, bijkomende voorwaarden

Op grond van artikel 9 lid 4 AVG kunnen lidstaten bijkomende voorwaarden opleggen voor de verwerking van (onder meer) genetische gegevens. In de consultatieversie van de Uitvoeringswet AVG bevat artikel 24 dergelijke bijkomende voorwaarden. Volgens dit artikel mogen genetische gegevens slechts in twee gevallen worden verwerkt, te weten: a) als een zwaarwegend geneeskundig belang daartoe noopt; of b) indien de verwerking noodzakelijk is ten behoeve van wetenschappelijk onderzoek of statistiek én de betrokkene uitdrukkelijk toestemming heeft gegeven. Op basis van deze bepaling zouden genetische gegevens dus alleen op basis van een uitdrukkelijke toestemming in wetenschappelijk onderzoek gebruikt mogen worden. Hoewel hierover veel discussie bestaat,[73] ligt aan dit relatief strikte regime voor de verwerking van genetische gegevens de gedachte ten grondslag dat genetische gegevens extra bescherming behoeven ten opzichte van andere bijzondere persoonsgegevens.

5.6 Deelconclusie

Uit het voorgaande blijkt dat artikel 9 lid 2 sub j AVG voornamelijk open normen bevat die een nadere invulling vergen in EU- of lidstatelijk recht. Daarbij gaat het ten eerste om het respecteren van de beginselen van noodzakelijkheid en evenredigheid. Uit het wetgevingsproces, de literatuur en erkende ethische normen blijken grote verschillen in visies op een wenselijke invulling van deze normen. Het is dan ook aannemelijk dat per lidstaat een ander regime tot stand zal komen, tenzij in EU-recht alsnog een aanvullende regeling volgt. Op grond van de consultatieversie van de Uitvoeringswet AVG zou het vragen van toestemming in Nederland de voorkeur houden. Uitzonderingen zijn immers slechts toegestaan voor zover het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning vergt. Bij de interpretatie van deze normen dient

73 Zie bijv. J.J.L. Chin en A.V. Campbell, 'What – if anything – is special about "genetic privacy"', in: *Genetic Privacy: An Evaluation of the Ethical and Legal Landscape*, Hackensack, NJ: Imperial College Press, 2013.

rekening te worden gehouden met digitale media die ingezet kunnen worden om grote groepen personen te bereiken, zoals communicatie per e-mail, portalen of andere interfaces. De omstandigheid dat het gaat om onderzoek onder grote groepen personen is dus op zichzelf onvoldoende om aan te nemen dat het vragen van toestemming een onevenredige inspanning vergt.
Ten tweede dient de uitzonderingsbepaling onderworpen te worden aan passende waarborgen en specifieke maatregelen. De enige concrete maatregelen of waarborgen genoemd in de AVG staan opgesomd in artikel 89 lid 1 AVG: waar mogelijk pseudonimisatie of anonimisatie van gegevens. Daarnaast dienen niet nader in de AVG omschreven specifieke maatregelen te worden getroffen én moet de wezenlijke inhoud van het recht op gegevensbescherming geëerbiedigd worden. Ook in de consulstatieversie van de Uitvoeringswet AVG ontbreekt een concretisering van de benodigde aanvullende passende en specifieke maatregelen. Dit gebrek aan harmonisatie zal niet bijdragen tot de uitwisseling van bijzondere persoonsgegevens tussen EU-lidstaten zonder toestemming van de betrokkene. Daar staat tegenover dat de open normen wel ruimte bieden voor een flexibele normontwikkeling op nationaal niveau, waarbij niet alleen wetgeving maar ook (ethische) richtlijnen een belangrijke rol kunnen spelen. Voor de gevallen waarin een uitzondering op het toestemmingsvereiste is toegestaan, kan bij de invulling van passende en specifieke maatregelen bijvoorbeeld gedacht worden aan het in stand houden van een laagdrempelig en effectief geen-bezwaarsysteem,[74] waardoor de uitoefening van het recht van bezwaar op grond van artikel 21 AVG wordt gefaciliteerd. Daarnaast kan voorafgaande toetsing door een ethische commissie overwogen worden, zoals de CIOMS Guidelines en Declaration of Taipei aanbevelen. Dit met name als het gaat om het bieden van toegang tot gegevensverzamelingen die vanwege hun aard of omvang bijzondere bescherming verdienen.

6 Beginselen en individuele rechten

Hoewel in het voorgaande met name het beginsel van rechtmatigheid centraal stond, kunnen ook andere beginselen, zoals die van doelbinding en opslagbeperking, op gespannen voet staan met een effectief gebruik van big data in gezondheidsonderzoek. Hetzelfde geldt voor een aantal van de rechten van betrokkenen die volgens het algemene regime van gegevensbescherming gelden. Om te voorkomen dat de verwerking voor onderzoeksdoeleinden hierdoor in onevenredige mate beperkt wordt, laat de AVG ruimte voor afwijkingen van een aantal van deze beginselen en rechten.

74 Zie hierover in relatie tot art. 7:457 en 7:458 BW: Ploem, 2010, p. 186.

6.1 *Afwijkingen van beginselen*

Het hergebruik van persoonsgegevens in gezondheidsonderzoek wordt gefaciliteerd door de afwijkingen van de beginselen van doelbinding en opslagbeperking. De verdere verwerking voor onderzoeksdoeleinden wordt op grond van artikel 5 lid 1 sub b AVG niet als onverenigbaar beschouwd met de oorspronkelijke doeleinden. Voorts bepaalt artikel 5 lid 1 sub e AVG dat gegevens voor onderzoeksdoeleinden voor langere perioden mogen worden opgeslagen. Voor deze beide uitzonderingen geldt dat de verwerking in overeenstemming moet zijn met artikel 89 lid 1 AVG en de vereiste technische en organisatorische maatregelen worden getroffen.[75]
Van de overige beginselen in artikel 5 AVG is de verwerking voor onderzoeksdoeleinden niet expliciet uitgezonderd. Dit betekent dat de beginselen van rechtmatigheid, behoorlijkheid en transparantie, minimale gegevensverwerking, juistheid, integriteit en vertrouwelijkheid en de verantwoordingsplicht geëerbiedigd moeten worden bij de verwerking voor onderzoeksdoeleinden. Wel zijn diverse afwijkingen mogelijk van individuele rechten van betrokkenen die op voornoemde beginselen zijn gebaseerd.

6.2 Rechten met afwijkingen voor onderzoeksdoeleinden

Van sommige individuele rechten kan op grond van artikel 89 lid 2 AVG in het belang van onderzoek worden afgeweken, indien EU-recht of nationaal recht in een grondslag daartoe voorziet. Het gaat dan om afwijkingen van het recht op inzage (artikel 15 AVG), het recht op rectificatie (artikel 16 AVG), het recht op beperking van de verwerking (artikel 18 AVG) en het recht van bezwaar (artikel 21 AVG). Daarnaast voorziet de AVG zelf in de grondslagen om af te wijken van een tweetal andere individuele rechten. Hier gaat het om een afwijking van *the right to be forgotten* ofwel het recht op gegevenswissing (artikel 17 lid 3 sub d AVG) en een afwijking van het recht op informatie ex artikel 14 AVG (artikel 14 lid 5 sub b AVG). Dit laatstgenoemde recht op informatie is van toepassing indien de gegevens niet van de betrokkene zelf zijn verkregen.
Voor al deze afwijkingen van individuele rechten geldt dat deze moeten voldoen aan de beginselen van noodzakelijkheid en evenredigheid. Afwijkingen zijn alleen toegestaan indien en voor zover de individuele rechten de verwerking voor onderzoeksdoeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren.[76]
Daarnaast moet iedere afwijking in overeenstemming zijn met artikel 89 lid 1 AVG en moeten de in dat artikellid bedoelde maatregelen worden getroffen. Specifiek voor de afwijking van het recht op informatie in artikel 14 AVG geldt nog dat aanvullende passende maatregelen moeten worden getroffen, 'waaronder het

75 Zie par. 5.3 over art. 89 lid 1 AVG.
76 Zie art. 14 lid 5 sub b, 17 lid 3 sub d en 89 lid 2 AVG.

openbaar maken van de informatie'. Dit openbaar maken van de informatie kan niet anders dan in algemene termen gebeuren, bijvoorbeeld op een website.
In de consultatieversie van de Uitvoeringswet AVG wordt de inhoud van artikel 44 Wbp, behoudens een taalkundige wijziging, gehandhaafd. Dit heeft tot gevolg dat afwijkingen van de artikelen 15, 16 en 18 AVG zijn toegestaan.[77] Hoewel daarnaast aan de in artikel 89 lid 1 en 2 AVG genoemde voorwaarden moet worden voldaan, wordt dit niet expliciet benadrukt in de consultatieversie van de Uitvoeringswet AVG. Op het recht van bezwaar in artikel 21 AVG is bewust geen afwijking geformuleerd. Dit zou betekenen dat de betrokkene onverkort op grond van artikel 21 AVG bezwaar kan maken om redenen die verband houden met zijn specifieke situatie. Van dit recht kan op grond van artikel 21 lid 6 AVG slechts worden afgeweken voor onderzoeksdoeleinden als dit noodzakelijk is voor de uitvoering van een taak van algemeen belang.

6.3 Rechten zonder afwijkingen voor onderzoeksdoeleinden

Individuele rechten waarop geen specifieke afwijkingen voor de verwerking voor onderzoeksdoeleinden zijn toegestaan, zijn het recht op informatie ex artikel 13 AVG, de kennisgevingsplicht,[78] het recht op overdraagbaarheid en het recht om niet te worden onderworpen aan geautomatiseerde besluitvorming.[79]
Bijzondere aandacht verdient het recht op informatie zoals neergelegd in artikel 13 AVG. Deze bepaling formuleert een informatieplicht voor de verantwoordelijke, voor de gevallen waarin de gegevens bij de betrokkene zelf worden verzameld. Het gaat onder meer om informatie over de verantwoordelijke en de functionaris voor gegevensbescherming, de verwerkingsdoeleinden en de rechtsgrond voor de verwerking, de ontvangers van persoonsgegevens, de periode van opslag en de rechten van de betrokkene.[80] De informatieplicht is volgens artikel 13 AVG slechts niet van toepassing indien en voor zover de betrokkene al over voornoemde informatie beschikt. Verwarrend is echter dat overweging 62 van de AVG op het eerste gezicht ruimte lijkt te bieden voor een ruimere uitzondering voor onderzoeksdoeleinden. In deze overweging is immers opgenomen dat informatieverstrekking niet noodzakelijk is indien deze onmogelijk blijkt of onevenredig veel inspanning zou vergen, waarbij in het bijzonder gedoeld wordt op de verwerking voor onderzoeksdoeleinden. Het is echter onduidelijk of deze overweging ook ziet op de informatieplicht ex artikel 13 AVG. Een interpretatie conform deze overweging vindt naar mijn inzicht geen steun in de tekst van artikel 13 AVG. De overweging lijkt dan ook eerder betrekking te hebben op de afwijking van de informatieplicht ex artikel 14 AVG, zoals omschreven in artikel 14 lid 5 sub b AVG.

---

77 Consultatieversie Uitvoeringswet AVG, art. 42 en p. 89-90.
78 Art. 19 AVG.
79 Art. 20 en 22 AVG.
80 Art. 13 lid 1 en 2 AVG.

Zodra de gegevens verder verwerkt worden voor een ander doel, dient in beginsel alle relevante informatie vooraf aan de betrokkene te worden verstrekt op grond van artikel 13 lid 3 AVG. In geval van verdere verwerking voor onderzoeksdoeleinden is het echter verdedigbaar dat deze informatieplicht niet onverkort geldt. De afwijking van het beginsel van doelbinding in artikel 5 lid 1 sub b AVG gaat namelijk uit van de fictie dat de verdere verwerking voor wetenschappelijk onderzoek niet onverenigbaar is met de oorspronkelijke doeleinden. Hergebruik voor (andere) onderzoeksdoeleinden lijkt daarom niet te kwalificeren als een verdere verwerking voor een ander doel zoals bedoeld in artikel 13 lid 3 AVG. Hierbij geldt dan wel de eis dat de verdere verwerking voldoet aan de voorwaarden in artikel 89 lid 1 AVG. Voorts is het onduidelijk of de informatieplicht voortduurt nadat de gegevens zijn verzameld indien voornoemde details wijzigen, zoals de contactgegevens van de verantwoordelijke. Indien het gaat om een voortdurende informatieplicht op detailniveau, kan dit een aanzienlijke administratieve belasting betekenen voor organisaties die gegevens langdurig onder zich houden.[81]

6.4 Deelconclusie

Een discussie die zich beperkt tot de onderwerpen anonimiteit en (uitzonderingen op) het toestemmingsvereiste doet geen recht aan het meeromvattende regime van gegevensbescherming. Het beginsel van rechtmatigheid is immers slechts één onderdeel van dit regime, naast de overige in artikel 5 AVG genoemde beginselen en de daarop gebaseerde regels en individuele rechten. De afwijkingen van een deel van deze algemene beginselen en individuele rechten lijken het gebruik van persoonsgegevens in data-intensief gezondheidsonderzoek voldoende te faciliteren. Voor een belangrijk deel van deze afwijkingen is wel vereist dat nationale wetgevers en/of de EU gebruikmaken van de ruimte die de AVG biedt om deze te verankeren in het recht. Of de verwerking ook op een verantwoorde manier plaats zal vinden, hangt in het bijzonder af van de invulling van de waarborgen en maatregelen die op grond van artikel 89 lid 1 AVG vereist zijn.
Op de informatieplicht ex artikel 13 AVG en het recht van bezwaar zijn nagenoeg geen afwijkingen voor onderzoeksdoeleinden toegestaan, indien de consultatieversie van de Uitvoeringswet AVG in ongewijzigde vorm wordt aangenomen. Een dergelijke combinatie van rechten zou in een geen-bezwaarsysteem resulteren, dat voor iedere verwerking van persoonsgegevens die van de betrokkene zelf verkregen worden, geldt. Bij de informatieverstrekking op grond van artikel 13 AVG dient de betrokkene immers geïnformeerd te worden over zijn rechten, waaronder het recht van bezwaar, ook als niet om toestemming hoeft te worden gevraagd.

81 Wellcome Trust, 2016.

7 Conclusie

Alles overziend lijkt de AVG data-intensief gezondheidsonderzoek niet onnodig of disproportioneel te belemmeren. Ook draagt de AVG op hoofdlijnen bij aan een overkoepelend systeem van bescherming op basis waarvan dit onderzoek op een verantwoorde manier plaats kan vinden. De EU-wetgever heeft echter de centrale doelstelling van harmonisatie in zeer beperkte mate bereikt inzake de regels die specifiek zien op de verwerking voor onderzoeksdoeleinden. Dit gebrek aan harmonisatie komt tot uiting in de machtiging in de AVG van lidstaten om in uitzonderingen te voorzien ten behoeve van wetenschappelijk onderzoek. Deze uitzonderingen betreffen bijvoorbeeld het alternatief voor het toestemmingsvereiste ex artikel 9 lid 2 sub j AVG en de afwijkingen van individuele rechten voor onderzoeksdoeleinden ex artikel 89 lid 2 AVG. Het ligt niet in de lijn der verwachting dat dergelijke uitzonderingen op korte termijn alsnog in EU-recht verankerd zullen worden. Het is daarom aan de lidstaten om hiervoor in nationaal recht een basis te bieden, bij gebreke waarvan voornoemde uitzonderingen niet zijn toegestaan. Bovendien zijn de voorwaarden en waarborgen – waar de uitzonderingen ten behoeve van onderzoek aan moeten worden onderworpen – onvoldoende specifiek omschreven in de AVG om tot een coherente bescherming te komen in de EU. Het risico is dan ook groot dat het negatieve effect op data-intensief gezondheidsonderzoek als gevolg van het gebrek aan rechtseenheid in de EU voorlopig blijft bestaan.
Positief is dat de AVG voldoende ruimte biedt voor een regime van gegevensbescherming specifiek gericht op wetenschappelijk onderzoek. Dit door de combinatie van uitzonderingen en afwijkingen ten behoeve van onderzoek met het vereiste dat in passende en specifieke voorwaarden en waarborgen wordt voorzien. Voor wat betreft deze waarborgen benadrukt de AVG sterk het belang bij governancemaatregelen. De AVG bevat, naast dataminimalisatie, echter weinig concrete aanwijzingen voor de invulling van deze maatregelen. Dit kan nadelige gevolgen hebben voor de bescherming van de rechten en belangen van betrokkenen, omdat deze voor een belangrijk deel afhangt van de governancemaatregelen. Hierbij gaat het in het bijzonder om de verwerkingen op basis van broad consent of een uitzonderingsbepaling conform artikel 9 lid 2 sub j AVG. De nadere invulling van deze governancemaatregelen is daarom een onderwerp dat nadere aandacht behoeft, ook van de nationale wetgever. Daarbij kan aansluiting worden gezocht bij de concrete en specifieke ethische normen in de recente CIOMS Guidelines of de WMA Declaration of Taipei. Het is dan wel van belang dat een passende keuze wordt gemaakt tussen statische wet- en regelgeving en meer flexibele normering in richtlijnen. Hierbij kan door de wetgever als gulden middenweg worden overwogen om een door de Autoriteit Persoonsgegevens goedgekeurde richtlijn te verplichten voor bepaalde verwerkingen voor onderzoeksdoeleinden. Deze verplichting zou beperkt kunnen worden tot verwerkingen voor onderzoeksdoeleinden op basis van een alternatief voor het toestemmingsvereiste conform artikel 9 lid 2 sub j AVG. Een dergelijke verplichting zou de vrij-

blijvendheid van een nadere invulling van passende en specifieke maatregelen wegnemen, terwijl de flexibiliteit van normstelling middels richtlijnen die ontstaan vanuit het veld niet verloren gaat.

Literatuur

Barocas en Nissenbaum (2014)
S. Barocas, H. Nissenbaum. 'Big data's end run around anonymity and consent', in: J. Lane et al. (eds.), *Privacy, big data, and the public good: Frameworks for Engagement*, Cambridge: Cambridge University Press, 2014.

Chin en Campbell (2013)
J.J.L. Chin en A.V. Campbell, 'What – if anything – is special about "genetic privacy"', in: T.S. Kaan en C.W. Ho (eds.), *Genetic Privacy: An Evaluation of the Ethical and Legal Landscape*, Hackensack, NJ: Imperial College Press, 2013.

CIOMS (2016)
CIOMS International Ethical Guidelines for Health-related Research Involving Humans, 2016, http://www.cioms.ch/ethical-guidelines-2016/ (d.d. 09-12-2016).

Delden en Van der Graaf (2016)
J.J.M. van Delden, R. van der Graaf, 'Revised CIOMS International Ethical Guidelines for Health-Related Research Involving Humans', *JAMA*, 2016. doi:10.1001/jama.2016.18977.

Dove, Thompson en Knoppers (2016)
E.S. Dove, B. Thompson, B.M. Knoppers, 'A step forward for data protection and biomedical research', *The Lancet*, 2016;387:1374–5.

Europees Parlement (2014)
Europees Parlement, wetgevingsresolutie van 12 maart 2014 over het voorstel voor een algemene verordening gegevensbescherming, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN (d.d. 09-12-2016).

Gymrek (2013)
M. Gymrek et al., 'Identifying personal genomes by surname inference', *Science* 2013;339:321-4.

ICER (2014)
ICER, http://www.minbuza.nl/binaries/content/assets/ecer/ecer/import/icer/handleidingen/2014/icer-handleiding-nationale-toetsing-eu-handvest-grondrechten.pdf (d.d. 09-12-2016).

Kaye et al. (2014)
J. Kaye, E.A. Whitley, D. Lund, M. Morrison, H. Teare, K. Melham, 'Dynamic consent: a patient interface for twenty-first century research networks', *European Journal of Human Genetics*, 2014;23:141–146.

Knoppers, Zawati en Kirby (2012)
B.M. Knoppers, M.H. Zawati, E.S. Kirby: 'Sampling populations of humans across the world: ELSI issues', *Annu Rev Genomics Hum Genet* 2012;13:395-413.

Lowrance (2012)
W.W. Lowrance: *Privacy, Confidentiality, and Health Research*, Cambridge University Press: Cambridge, UK, 2012, p. 158.

Moerel en Prins (2016)
E.M.L. Moerel, J.E.J. Prins, 'Privacy voor de homo digitalis', in: *Homo digitalis. Preadviezen NJV 2016-1*, Wolters Kluwer, 2016.

Mostert et al. (2016)
M. Mostert, A.L. Bredenoord, M.C.I.H. Biesaart, J.J.M. van Delden, 'Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach', *European Journal of Human Genetics*, 2016;24:956-60.

Nature Biotechnology (2015)
'Apple's ResearchKit frees medical research', *Nature Biotechnology*, 2015;33:322.

Nuffield Council on Bioethics (2015)
Nuffield Council on Bioethics, 'The collection, linking and use of data in biomedical research and healthcare: ethical issues', 2015, p. 146-149, http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf (d.d. 24-12-2016).

Ottes (2016)
L. Ottes, 'Big Data in de zorg', Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid, 2016, Working Paper 19.

Ploem (2004)
M.C. Ploem, *Tussen privacy en wetenschapsvrijheid, Regulering van gegevensverwerking voor medisch-wetenschappelijk onderzoek*, Den Haag: Sdu Uitgevers, 2004.

Ploem (2010)
M.C. Ploem, 'Gegeven voor de wetenschap, Regulering van onderzoek met gegevens, lichaamsmateriaal en biobanken', in: *Wetenschappelijk onderzoek in de zorg, Preadvies 2010 Vereniging voor Gezondheidsrecht*, Den Haag: Sdu Uitgevers, 2010.

Ploem, Essink-Bot en Stronks (2013)
M.C. Ploem, M.L. Essink-Bot, K. Stronks, 'Proposed EU data protection regulation is a threat to medical research', *British Medical Journal*, 2013;346:f3534.

Ploem en Dute (2016)
M.C. Ploem en J.C.J. Dute, 'Wetenschappelijk onderzoek na overlijden: goed geregeld?', *TvGR*, 2016;8:498-512.

Quinn (2016)
P. Quinn, 'The Anonymisation of Research Data — A Pyric Victory for Privacy that Should Not Be Pushed Too Hard by the EU Data Protection Framework?', *European Journal of Health Law*, 2016;24:1-24;

Raad van Ministers (2015)
Raad van Ministers, goedkeuring op 11 juni 2015 van het voorstel voor een algemene verordening gegevensbescherming, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf (d.d. 09-12-2016).

Rodriquez (2013)
L.L. Rodriguez et al., 'Research ethics. The complexities of genomic identifiability' *Science* 2013;339:275-6;

Savage (2016)
N. Savage, 'The Myth of Anonimity', *Nature*, 2016;537:70-2.

Sluyters en Biesaart (1995)
B. Sluyters en M.C.I.H. Biesaart, *De geneeskundige behandelingsovereenkomst na invoering van de WGBO*, Zwolle: W.E.J. Tjeenk Willink, 1995.

Tene en Polonetsky (2012)
O. Tene, J. Polonetsky, 'Privacy in the age of Big Data: a time for big decisions', *Stanford Law Rev Online* 2012;64:63–9.

Van Veen (2013)
E.B. van Veen, 'Europe and tissue research: a regulatory patchwork', *Diagn Histopathol*, 2013;19:331–6.

Wellcome Trust (2016)
Wellcome Trust, 'Analysis: Research and the General Data Protection Regulation': https://wellcome.ac.uk/sites/default/files/new-data-protection-regulation-key-clauses-wellcome-jul16.pdf (d.d. 09-01-2016).

WMA (2016)
WMA Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks, 2016, http://www.wma.net/en/30publications/10policies/d1/ (d.d. 09-12-2016).

PREADVIEZEN VERENIGING VOOR GEZONDHEIDSRECHT (1968-2016)

(1968 tm 2003 indien voorradig tegen kostprijs en verzendkosten beschikbaar via VGR-secretariaat, tel. 030 - 28 23 848, e-mail: vgr@fed.knmg.nl, vanaf 2004 te bestellen via Sdu Klantenservice te Den Haag, tel. 070 - 378 98 80, e-mail: sdu@sdu.nl)

1968 H.J.J. Leenen: Gezondheidsrecht – een poging tot plaatsbepaling.*
Verder het rapport van de Commissie herziening interne rechtspraak van de KNMG *

1969 C.J. Goudsmit: Voordracht over problemen rond de wetgeving van geestelijk gestoorden. Daaraan werd nog een tweede vergadering gewijd.*

1970 J.M.M. Maeijer: De aansprakelijkheid voor handelingen van een medisch team.*

1971 W.B. van der Mijn: Wetgeving medische beroepsuitoefening.*

1972 J.Ch. Cornelis en A.S. Frowijn: De ontwikkeling van de wetgeving op het gebied van de organisatie van de gezondheidszorg.*

1973 B. Sluyters: Medische aansprakelijkheid in Amerika en Nederland.*
Tijdens deze vergadering werd ook het rapport van de werkgroep juridische aspecten van de relatie ziekenfondsmedewerkers – verzekerde o.l.v. T.J.S. Postma besproken.*

1974 M. Rood-de Boer: De positie van de minderjarige in de gezondheidszorg.*

1975 J. ter Heide: Dwang en drang in de medische behandeling.*

1976 H.J.J. Leenen: Milieuhygiënerecht.*

1977 H.P. Utermark: Medisch Tuchtrecht.*

1978 A.E. Leuftink en N. de Jong: De rechtspositie van de keurling.*

1979 Advies inzake registratie van medische en psychologische gegevens en de bescherming van de persoonlijke levenssfeer (privacy) van de Gezondheidsraad, becommentarieerd door F. Kuitenbrouwer, L. Kortbeek en E. Dil-Stork.*

1980 Het selectievraagstuk in de gezondheidszorg; het selecteren van patiënten bij schaarste van behandelingsmogelijkheden voorbereid door vier personen, te weten S.A. de Lange, H.E. Nicolaï, P.C. Sporken en H.F. Visser-'t Hooft. *
Werkgroep richtlijnen keuringen: Wat mag en wat moet bij een aanstellingskeuring.

1981 M.N.G. Dukes: De toelating van geneesmiddelen in Nederland.*

1982 P.J.W. de Brauw: Beschouwingen over samenwerking in de geneeskundige behandeling en verzorging van patiënten.
Co-referaat van een medische werkgroep bij het preadvies;
Beschouwingen over samenwerking in de geneeskundige behandeling en verzorging van patiënten.

1983 H.A. Brasz en D.W.P. Ruiter: Het plansysteem van de Wet voorzieningen gezondheidszorg.*

1984 H.D.C. Roscam Abbing: Overheid en het recht op gezondheidszorg.

1985 C. Kelk: Klagen of kwijnen. De rechten van verpleeghuispatiënten en de behandeling van hun klachten.*

1986 J.C.M. Leyten: Welzijn, vrijheid en dwang.

1987 J.K.M. Gevers: Juridische aspecten van erfelijkheidsonderzoek en -advies.

1988 J.P. Kasdorp: Grenzen aan het recht op gezondheidszorg.

1989 B. Sluyters en H.R.G. Feber: De gezondheidszorg en het strafrecht.

1990 F.C.B. van Wijmen: Driehoeksverhoudingen. Gezondheidsrechtelijke beschouwingen over vertegenwoordiging van meerderjarige onbekwamen.

1991 J.H. Hubben: Kwaliteit en recht in de gezondheidszorg.

1992 Jubileumcongres 25 jaar Vereniging voor Gezondheidsrecht:
J.H. Hubben en H.D.C. Roscam Abbing (red.), Gezondheidsrecht in perspectief. De Tijdstroom Utrecht 1993.*

1993 H.D.C. Roscam Abbing: Patiënt en gezondheidszorg in het recht van de Europese Gemeenschap.*

1994 J. Legemaate: Goed recht. De betekenis en de gevolgen van het recht voor de praktijk van de hulpverlening.

1995 E.T.M. Olsthoorn-Heim en L. Bergkamp: Medisch wetenschappelijk onderzoek: Lichaamsmateriaal voor de wetenschap en het wetsvoorstel medische experimenten.*

1996 E.W. Roscam Abbing en J.K.M. Gevers: Voorspellend Medisch Onderzoek: Mogelijkheden, verwachtingen en toegang; Rechtsbescherming.*

1997 H.J.J. Leenen: Recht op zorg voor de gezondheid.*

1998 C. Kelk: Gezondheidszorg voor gedetineerden.*

1999 P.J. Hustinx: Informatietechnologie in de gezondheidszorg.*

2000 F.C.B. van Wijmen: Richtlijnen voor verantwoorde zorg.
Over de betekenis van standaardisering voor patiënt,
professional en patiëntenzorg.

WGBO en bedrijfsarts: Advies uitgebracht aan de besturen van de Vereniging voor Gezondheidsrecht en de Nederlandse Vereniging voor Arbeids- en Bedrijfsgeneeskunde. Werkgroep WGBO en bedrijfsarts. VGR-najaarsvergadering 2000.

2001 Th.A.M. te Braake en L.E. Kalkman-Bogerd: Procreatietechnologie en recht. Toelaatbaarheid en regulering van IVF-onderzoek; Van kinderwens tot ouderschap.

2002 H.D.C. Roscam Abbing, J. Legemaate en G.R.J. de Groot: Zorg, schaarste en recht.
– Solidariteit en individuele vrijheid; vrijheid in gebondenheid
– De (dubbel)rol van de arts
– Verantwoordelijkheid en aansprakelijkheid voor tekorten in de zorg.

Jubileumbundel: Omzien naar de toekomst, 35 jaar preadviezen Vereniging voor Gezondheidsrecht. Redactie: J.C.J. Dute, J.K.M. Gevers en G.R.J. de Groot.*

2003 T.P. Widdershoven en K. Blankman: Psychiatrie en Recht.
– De Wet Bopz en de psychiatrie. Kanttekeningen bij een regeling
– Rechtsbescherming bij vrijheidsbeneming in de sectoren verstandelijk gehandicaptenzorg en psychogeriatrie.

2004 E.-B. van Veen, E.J.C. de Jong en W.R. Kastelein: Het beroepsgeheim, continuïteit en verandering.*
– Het beroepsgeheim in de individuele gezondheidszorg
– Het beroepsgeheim en derdenbelangen
– Het beroepsgeheim in rechte. Zwijgen: recht of plicht?
ISBN: 978-90-12-09999-8 Sdu

2005 W. van den Ouwelant en J.C.J. Dute: Preventieve Gezondheidszorg.*
– Heilzame wetten. Historie, karakter, plaats en vorm van de publieke gezondheidszorg
– Infectieziekten, dwang en drang
ISBN: 978-90-12-10757-0 Sdu

2006 J.A. Lisman, M.F. van der Mersch en C. Velink: Geneesmiddelen en Recht.
– De toelating van geneesmiddelen. Hoe effectief is ons systeem?
– Het recht op geneesmiddelen. Hoe kosten de zorg beheersen
ISBN: 978-90-12-11313-7 Sdu

2007 P.C. Ippel, T. Hartlief en P.A.M. Mevis: Gezondheidsrecht: betekenis en positie.
– Het gewicht van het gezondheidsrecht
– De staat van het privaatrechtelijke gezondheidsrecht
– Gezondheidsrecht en strafrecht; ontwikkelingen in een niet altijd gemakkelijke relatie.
ISBN: 978-90-12-12028-9 Sdu

2008 J.H.H.M. Dorscheidt en A.C. de Die: De toekomst van de Wet BIG.
– Taakherschikking en verantwoordelijkheidsverdeling
– Gewaarborgde kwaliteit
ISBN: 978-90-12-38014-0 Sdu

2009 A.C. Hendriks, J.W. van de Gronden en J.J.M. Sluijs: Gezondheidszorg en Europees recht
– De betekenis van het EVRM voor het gezondheidsrecht
– De betekenis van het EG-verdrag voor het reguleren van de zorgmarkt
ISBN: 978-90-12-38187-1 Sdu

2010 D.P. Engberts, Y.M. Koster en M.C. Ploem: Wetenschappelijk onderzoek in de zorg
– De juridische normering van medisch-wetenschappelijk onderzoek met mensen
– Gegeven voor de wetenschap – *Regulering van onderzoek met gegevens, lichaamsmateriaal en biobanken*
ISBN: 978-90-12-38354-7 Sdu

2011 J.G. Sijmons, T.A.M. van den Ende, G.R.J. de Groot: Stelsel onder stress
– De cure: transitie en onbalans
– De care: voortvarend na bedachtzaam wegen
– De schuivende panelen van de zorgverzekering
ISBN: 978-90-12-38577-0 Sdu

2012 Oratiebundel Gezondheidsrecht. Verzamelde redes 1971 – 2011
40 jaar Nederlands gezondheidsrecht in een twintigtal oraties
t.g.v. 45-jarig bestaan VGR
ISBN: 978-90-12-38840-5 Sdu

2013 J.L. Smeehuizen, A.J. Akkermans en T. Vansweevelt: Ontwikkelingen rond medische aansprakelijkheid.
– Medische aansprakelijkheid: over grote problemen, haalbare verbeteringen en overschatte revoluties
– Ontwikkelingen rond medische aansprakelijkheid in België
ISBN 978-90-12-39081-1 Sdu

2014 G.A. den Hartogh en P.B. Cliteur: Ethiek en Gezondheidsrecht
– De morele grondslagen van het gezondheidsrecht: de erfenis van Leenen
– Morele en immorele religieus gelegitimeerde praktijken in het gezondheidsrecht
ISBN 978-90-12-39300-3 Sdu

2015 E. Steyger, J.J. Rijken, M.F. Vermaat, E. Plomp, T.A.M. van den Ende: Op weg naar 10 jaar nieuw zorgstelsel. Terug- en vooruitblik.
– Het zorgstelsel in Europeesrechtelijk perspectief
– Concurrentie tussen zorgaanbieders: de klant is koning, maar wie is de klant?
– Vertrouwen komt te voet
– De introductie van ziekenhuizen met winstoogmerk
– Zorgfraude: van handhaving en hoe systemen hun eigen ongelukken genereren
ISBN 978-90-12-39544-1 Sdu

2016 M.J.M.H. Lombarts, A.C. de Die, H.C. van Eyck van Heslinga MMV, A. Hammerstein: Functioneren en disfunctioneren van professionales in de zorg
– Funstioneren en disfunctioneren van bestuurders
– De zorginstelling heeft een professionele toezichthouder nodig
ISBN 978-90-12-39756-8 Sdu

* niet meer voorradig